# DOCUMENT RESUME

ED 149 734 IR 005 517

| | |
|---|---|
| AUTHOR | Ruthberg, Zella G. |
| TITLE | Audit and Evaluation of Computer Security. Computer Science and Technology. |
| INSTITUTION | National Bureau of Standards (DOC), Washington, D.C. Inst. for Computer Sciences and Technology. |
| REPORT NO | SP 500-19 |
| PUB DATE | Oct 77 |
| NOTE | 253p.; Proceedings of the NBS Invitational Workshop (Miami Beach, Florida, March 22-24, 1977) |
| AVAILABLE FROM | Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402 (Stock No. 003-003-01848-1, $4.00) |
| EDRS PRICE | MF-$0.83 HC-$14.05 Plus Postage. |
| DESCRIPTORS | Administrator Responsibility; *Computers; Computer Science; *Data Bases; Evaluation Methods; Futures (of Society); Information Processing; Information Systems; Physical Design Needs; *Security (Psychology); Standards; *State of the Art Reviews |

ABSTRACT

This is a collection of consensus reports, each produced at a session of an invitational workshop sponsored by the National Bureau of Standards. The purpose of the workshop was to explore the state-of-the-art and define appropriate subjects for future research in the audit and evaluation of computer security. Leading experts in the audit and computer communities were invited. Ten topics are reported on: (1) internal audit standards, (2) qualifications and training, (3) security administration, (4) audit considerations in various system environments, (5) administrative and physical controls, (6) program integrity, (7) data integrity, (8) communications, (9) post-processing audit tools and techniques, and (10) interactive audit tools and techniques. (Author)

***********************************************************************
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
***********************************************************************

ED149734

## COMPUTER SCIENCE & TECHNOLOGY:

000384

# Audit and Evaluation of Computer Security

Proceedings of the NBS Invitational Workshop
held at Miami Beach, Florida, March 22-24, 1977

U.S. DEPARTMENT OF HEALTH,
EDUCATION & WELFARE
NATIONAL INSTITUTE OF
EDUCATION

THIS DOCUMENT HAS BEEN REPRODUCED EXACTLY AS RECEIVED FROM THE PERSON OR ORGANIZATION ORIGINATING IT. POINTS OF VIEW OR OPINIONS STATED DO NOT NECESSARILY REPRESENT OFFICIAL NATIONAL INSTITUTE OF EDUCATION POSITION OR POLICY

Edited by:

Zella G. Ruthberg

Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D. C. 20234

Robert G. McKenzie

General Accounting Office
Washington, D. C. 20548

Session Chairpersons;

William E. Perry
C. O. Smith
Blake Greenlee
Carl Hammer
W. H. Murray
Clark Weissman
Leonard I. Krauss
Jerry FitzGerald
Richard D. Webb
Hart J. Will

U.S. DEPARTMENT OF COMMERCE, Juanita M. Kreps, Secretary
Dr. Sidney Harman, Under Secretary
Jordan J. Baruch, Assistant Secretary for Science and Technology
NATIONAL BUREAU OF STANDARDS, Ernest Ambler, Acting Director

Issued October 1977

IR005517

## Reports on Computer Science and Technology

The National Bureau of Standards has a special responsibility within the Federal Government for computer science and technology activities. The programs of the NBS Institute for Computer Sciences and Technology are designed to provide ADP standards, guidelines, and technical advisory services to improve the effectiveness of computer utilization in the Federal sector, and to perform appropriate research and development efforts as foundation for such activities and programs. This publication series will report these NBS efforts to the Federal computer community as well as to interested specialists in the academic and private sectors. Those wishing to receive notices of publications in this series should complete and return the form at the end of this publication.

National Bureau of Standards Special Publication 500-19
Nat. Bur. Stand. (U.S.), Spec. Publ. 500-19, 256 pages (Oct. 1977)
CODEN: XNBSAV

Library of Congress Catalog Card Number: 77-600045

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1977

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402
Price $4—Stock No. 003-003-01848-1

# FOREWORD

The increasing use of computers by Government and private organizations for the storage and manipulation of records of all kinds--personal as well as of a business nature--has placed computers and the systems in which they reside in an extremely sensitive position in our society. The needs of the individual as well as Government and private organizations require that this data and their resident systems be accurate and reliable. These needs also require that this data and these systems be given adequate protection from threats and hazards. The establishment of secure computer systems is the way in which the computer community assures the users of such systems that all of these requirements are being met.

The auditing and evaluating of computer systems for adequate security has been a natural outgrowth of this widening interest in this area. Controls that provide computer security are of interest to both the financial and internal auditors and has been made a subject of special consideration by organizations such as the Institute of Internal Auditors, the American Institute of Certified Public Accountants, and the EDP Auditors Associtation.

The National Bureau of Standards, with the support of the U.S. General Accounting Office, sponsored an invitational workshop in March of 1977 to explore the subject of "Audit and Evaluation of Computer Security." Leading experts in the audit and computer communities were invited to share their thoughts and develop a consensus view on ten aspects of the subject. These Proceedings are the results of that meeting.

To all those concerned with the audit and evaluation of computer security today, we at the National Bureau of Standards offer this series of consensus reports for your consideration. The views expressed do not necessarily reflect those of the National Bureau of Standards, the U. S. General Accounting Office, or any of the organizations that sponsored an individual at the workshop. However, these reports do reflect the composite thoughts of a group that deserves your serious attention.

M Zane Thornton

M. Zane Thornton
Acting Director
Institute for Computer
Sciences and Technology

# PREFACE

The National Bureau of Standards (NBS) initiated a Task Group within the Federal Information Processing Standards (FIPS) program in 1973 to develop standards in Computer Systems Security. Task Group 15 (TG-15) was composed of representatives from private industry as well as Federal, State and local governments. The NBS Invitational Workshop on Audit and Evaluation of Computer Security was organized as one phase of a two-phase project defined by the Task Group in this important area of computer security. These Proceedings are the result of phase one. The second phase will be to adapt this information to the needs of Federal agencies in the form of Federal Information Processing Guidelines. This latter effort will be carried out by a working group convened for this purpose and will result in a FIPS publication by NBS.

The General Chairman and organizer of the Workshop was Robert G. McKenzie of the U.S. General Accounting Office. As leader of the TG-15 project on computer security auditing, he initiated and planned the Workshop and co-edited these Proceedings. Mr. McKenzie is an audit manager at GAO and has conducted a number of reviews of computer security of proposed and on-going systems in the Federal Government.

The General Vice-Chairman of the Workshop was Zella G. Ruthberg of the National Bureau of Standards. As NBS coordinator of the TG-15 security audit project, Mrs. Ruthberg worked closely with Mr. McKenzie on the planning, acted as the Workshop arrangements chairman, and is co-editor of these Proceedings. She has conducted a wide range of projects in computer science at NBS and most recently has become active in the managerial procedures required for computer security.

Mr. S. Jeffery, Chief of the Systems and Software Division of the Institute for Computer Sciences and Technology of NBS, headed the NBS staff at the Workshop. Mr. Jeffery has been active in the formulation of policy concerning the effective utilization of computers within the Federal Government and is manager of the computer program at NBS. This program provided the needed technical and administrative support for this Workshop.

I would like to thank all of the particitpants in this Workshop, the Chairmen and Recorders of the sessions, and the three individuals named above for the success of the Workshop. The products to be derived from the Workshop and subsequent efforts in this area will have far-reaching, beneficial effects on the use of computers throughout the country.

Dennis K. Branstad
Chairman, TG-15

## ABSTRACT

The National Bureau of Standards, with the support of the U.S. General Accounting Office, sponsored an invitational workshop on "Audit and Evaluation of Computer Security," held in Miami Beach, Florida on March 22-24, 1977. Its purpose was to explore the state-of-the-art in this area and define appropriate subjects for future research. Leading experts in the audit and computer communities were invited to discuss the subject in one of ten sessions, each of which considered a different aspect. A consensus report was produced by each of the ten sessions and these reports form the body of these Proceedings. The ten topics reported on are: Internal Audit Standards, Qualifications and Training, Security Administration, Audit Considerations in Various System Environments, Administrative and Physical Controls, Program Integrity, Data Integrity, Communications, Post-Processing Audit Tools and Techniques, and Interactive Audit Tools and Techniques.

KEYWORDS: Audit standards, audit techniques, audit tools, audit training, communications security, computer controls, computer security, data integrity, interactive audit, internal audit, post-processing audit, program integrity.

# ACKNOWLEDGEMENTS

The success of the Workshop was dependent on the work of many people. We would particularly like to take this opportunity to thank all the Session Chairmen, the Session Recorders, and the attendees for their efforts in behalf of this Workshop. We would also like to thank the session coordinators Robert V. Jacobson, John Panagacos, and Thomas C. Lowe for making things run smoothly while the Workshop was taking place; and Dennis K. Branstad for photographing scenes from the Workshop.

THE EDITORS

# TABLE OF CONTENTS

FOREWORD . . . iii

PREFACE . . . iv

EXECUTIVE SUMMARY . . . xix

PART I: INTRODUCTION . . . 1-1

- 1. HOST WELCOMING ADDRESS . . . 1-1
- 2. EDITORS' COMMENTS ON THE SESSIONS AND THE REPORTS . . . 1-3
  - 2.1 Some Definitions of Terms . . . 1-3
  - 2.2 Observations . . . 1-4
  - 2.3 Reading the Proceedings . . . 1-4

PART II: KEYNOTE ADDRESS . . . 2-1

- 1. INTRODUCTION . . . 2-2
- 2. AN APPROACH TO THE WORKSHOP . . . 2-2
- 3. COMMENTS ON PROPOSED TOPICS . . . 2-3
  - 3.1 Internal Audit Standards . . . 2-3
  - 3.2 Qualifications and Training . . . 2-3
  - 3.3 Security Administration . . . 2-4
  - 3.4 Audit Considerations in Various System Environments . . . 2-4
  - 3.5 Administrative and Physical Controls . . . 2-4
  - 3.6 Program Integrity . . . 2-4
  - 3.7 Data Integrity . . . 2-4
  - 3.8 Communications . . . 2-5
  - 3.9 Post-Processing Audit Tools and Techniques . . . 2-5
  - 3.10 Interactive Audit Tools and Techniques . . . 2-5

PART III: INTERNAL AUDIT STANDARDS . . . 3-1
EDITORS' NOTE . . . 3-2

Supplemental Standards for Internal Auditor's Expanded Role in Reviewing Computer Systems and Their Development . . . 3-3

- 1. INTRODUCTION . . . 3-3
  - 1.1 Automated Systems Effect on Environment . . . 3-3
  - 1.2 Computer Security Defined . . . 3-3
  - 1.3 Discussion of Audit Involvement in Computer Security . . . 3-4
  - 1.4 Changing Auditor Requirement . . . 3-5

2. SUPPLEMENTAL STANDARDS FOR COMPUTER INTERNAL AUDIT WORK . . . . . . . . . . 3-5
    2.1 General . . . . . . . . . . 3-5
    2.2 Supplemental Standard for Systems Development . . . 3-5
        2.2.1 Commentary . . . . . . . . . . 3-6
    2.3 Supplemental Standard for Operational Systems (Application Controls) . . . . . . . . . . 3-7
        2.3.1 Commentary . . . . . . . . . . 3-7
    2.4 Supplemental Standard for Physical Security and General Controls . . . . . . . . . . 3-8
        2.4.1 Commentary . . . . . . . . . . 3-8
    2.5 Other Audit Requirements . . . . . . . . . . 3-10

3. RECOMMENDED COURSE OF ACTION . . . . . . . . . . 3-10

4. REFERENCES . . . . . . . . . . 3-11

PART IV: QUALIFICATIONS AND TRAINING . . . . . . . . . . 4-1
EDITORS' NOTE . . . . . . . . . . 4-2

Qualifications and Training . . . . . . . . . . 4-3

o INTRODUCTION . . . . . . . . . . 4-3
o CONSIDERATIONS ASSOCIATED WITH DEVELOPING A COMMON BODY OF KNOWLEDGE . . . . . . . . . . 4-3
o THE EIGHT PARTS OF THE COMMON BODY OF KNOWLEDGE . . . . . 4-6

1. COMPUTER SYSTEM, OPERATIONS, AND SOFTWARE . . . . . . . . 4-6
2. DATA PROCESSING TECHNIQUES . . . . . . . . . . 4-7
3. MANAGEMENT OF THE DATA PROCESSING FUNCTION . . . . . . . . 4-7
4. SECURITY OF THE DATA PROCESSING FUNCTION . . . . . . . . 4-7
5. RISK ANALYSIS AND THREAT ASSESSMENT . . . . . . . . . . 4-8
6. MANAGEMENT CONCEPTS AND PRACTICES . . . . . . . . . . 4-8
7. AUDITING CONCEPTS AND PRACTICES . . . . . . . . . . 4-9
8. BASIC QUALIFICATIONS NEEDED TO EVALUATE COMUTER SECURITY . . . . . . . . . . 4-9

o OUTLINE OF THE COMMON BODY OF KNOWLEDGE . . . . . . . . . . 4-11
o BIBLIOGRAPHY . . . . . . . . . . 4-13

PART V: SECURITY ADMINISTRATION . . . . . . . . . . 5-1
EDITORS' NOTE . . . . . . . . . . 5-2

1. INTRODUCTION . . . . . . . . . . 5-3
    1.1 General . . . . . . . . . . 5-3
    1.2 Privacy Legislation . . . . . . . . . . 5-4
        1.2.1 The Privacy Act of 1974 . . . . . . . . . . 5-4
        1.2.2 Laws in Other Countries . . . . . . . . . . 5-4
        1.2.3 International Privacy Law Compatibility . . 5-5
    1.3 Organization of this Report . . . . . . . . . . 5-5

- 2. SECURITY ADMINISTRATION PROGRAM . . . . . 5-5
  - 2.1 Introduction . . . . . 5-5
  - 2.2 Planning by Management . . . . . 5-6
  - 2.3 Management Control . . . . . 5-7
  - 2.4 ADP Security . . . . . 5-9
    - 2.4.1 Administrative Security . . . . . 5-9
    - 2.4.2 Physical Security Administration . . . . . 5-11
    - 2.4.3 Technical Security . . . . . 5-14
    - 2.4.4 Training . . . . . 5-16
    - 2.4.5 A Suggested Security System for an On-Line System--An Example . . . . . 5-16
- 3. AUDITING THE SECURITY ADMINISTRATION FUNCTION . . . . . 5-18
  - 3.1 Organizational Requirements . . . . . 5-18
  - 3.2 The Audit Process . . . . . 5-19
- APPENDIX: SOME FEATURES OF THE FEDERAL GERMAN PRIVACY LAW . . . . . 5-21

PART VI: AUDIT CONSIDERATIONS IN VARIOUS SYSTEM ENVIRONMENTS . . 6-1
- EDITORS' NOTE . . . . . 6-2
- Audit Considerations in Various System Environments . . . . . 6-3
- 1. INTRODUCTION . . . . . 6-3
- 2. DEFINITIONS . . . . . 6-3
- 3. METHODOLOGY . . . . . 6-4
  - 3.1 Audit Versus Design . . . . . 6-4
  - 3.2 Steps the Design Team Must Take . . . . . 6-5
  - 3.3 Steps the Operational Auditor Must Take . . . . . 6-7
- 4. ENVIRONMENT AND CONTROL . . . . . 6-8
  - 4.1 Checklists . . . . . 6-11
  - 4.2 Guideline Book . . . . . 6-12
- 5. GUIDELINES . . . . . 6-13
- 6. CONCLUSIONS . . . . . 6-14
- APPENDIX: FOUR EXAMPLES . . . . . 6-16
- 1. SYSTEM SELECTION . . . . . 6-16
- 2. DETERMINATION OF ENVIRONMENT . . . . . 6-16
  - 2.1 Physical . . . . . 6-16
  - 2.2 Systems . . . . . 6-16
  - 2.3 Administrative . . . . . 6-17

3. IDENTIFICATION OF CONTROL TECHNIQUES . . . . . . . . . . . 6-17
  3.1 Physical . . . . . . . . . . . . . . . . . . . . . . 6-17
  3.2 Systems . . . . . . . . . . . . . . . . . . . . . . . 6-18
  3.3 Administrative . . . . . . . . . . . . . . . . . . . 6-18
4. CONTROL ANALYSIS . . . . . . . . . . . . . . . . . . . . . 6-18
5. COMPOSITE EVALUATION . . . . . . . . . . . . . . . . . . . 6-19

EXAMPLE NO. 1 General Purpose Multiuser Programming System 6-20
EXAMPLE NO. 2 Dedicated Data Base Management System . . . . 6-21
EXAMPLE NO. 3 Distributed Multiuser Remote Access System . 6-22
EXAMPLE NO. 4 Dedicated Batch-Dollar Disbursement System . 6-23

PART VII: ADMINISTRATIVE AND PHYSICAL CONTROLS . . . . . . . . . . 7-1
EDITORS' NOTE . . . . . . . . . . . . . . . . . . . . . . . . 7-2

Report of the Working Group on Administrative and Physical Controls . . . . . . . . . . . . . . . . . . . . . . . . 7-3

1. REVIEW OF THE CHARGE . . . . . . . . . . . . . . . . . . . 7-3

2. THE AUDITOR AND COMPUTER SECURITY . . . . . . . . . . . . 7-3

3. PROBLEMS . . . . . . . . . . . . . . . . . . . . . . . . . 7-5

4. SUGGESTIONS FOR THE AUDITOR . . . . . . . . . . . . . . . 7-6
  4.1 Audit Focus and Materiality . . . . . . . . . . . . . 7-7
  4.2 Standards of Practice and Their Documentation . . . 7-8
  4.3 The Security Audit Report . . . . . . . . . . . . . . 7-9

5. TYPES OF AUDITS . . . . . . . . . . . . . . . . . . . . . 7-10
  5.1 Introduction . . . . . . . . . . . . . . . . . . . . 7-10
  5.2 Checklists/References . . . . . . . . . . . . . . . . 7-11
  5.3 Approach . . . . . . . . . . . . . . . . . . . . . . 7-11

6. SYSTEMS DEVELOPMENT AND MAINTENANCE PRACTICES . . . . . . 7-12
  6.1 Concern . . . . . . . . . . . . . . . . . . . . . . . 7-12
  6.2 Purpose . . . . . . . . . . . . . . . . . . . . . . . 7-13
  6.3 Approach . . . . . . . . . . . . . . . . . . . . . . 7-13
  6.4 Scope . . . . . . . . . . . . . . . . . . . . . . . . 7-13
    6.4.1 Design Standards . . . . . . . . . . . . . . . . 7-13
    6.4.2 Organization Control . . . . . . . . . . . . . . 7-14
    6.4.3 Access Control . . . . . . . . . . . . . . . . . 7-14
    6.4.4 Phase Review/Project Control . . . . . . . . . . 7-15
    6.4.5 Testing/System Assurance . . . . . . . . . . . . 7-16
    6.4.6 Promotion Process . . . . . . . . . . . . . . . . 7-16
    6.4.7 Documentation . . . . . . . . . . . . . . . . . . 7-17
    6.4.8 Auditor/Independent Party Involvement . . . . . 7-17
    6.4.9 Configuration Management . . . . . . . . . . . . 7-17
    6.4.10 Emergency Procedures . . . . . . . . . . . . . . 7-18

7. APPLICATION REVIEW . . . . . . . . . . . . . . . . . . . . . . 7-18
  7.1 Concern . . . . . . . . . . . . . . . . . . . . . . 7-18
  7.2 Purpose . . . . . . . . . . . . . . . . . . . . . . 7-18
  7.3 Approach . . . . . . . . . . . . . . . . . . . . . . 7-19
  7.4 Scope . . . . . . . . . . . . . . . . . . . . . . 7-19
    7.4.1 Input/Output Controls . . . . . . . . . . . . 7-19
    7.4.2 System Internal Control Effectiveness . . . 7-19
    7.4.3 Separation of Duties . . . . . . . . . . . . 7-20
    7.4.4 Sensitive Program Controls . . . . . . . . . 7-20
    7.4.5 User Satisfaction/Involvement . . . . . . . . 7-20
    7.4.6 Report Utilization . . . . . . . . . . . . . 7-20
    7.4.7 System Documentation . . . . . . . . . . . . 7-20
    7.4.8 Vital Records . . . . . . . . . . . . . . . 7-21

8. INSTALLATION SECURITY . . . . . . . . . . . . . . . . . . . . 7-21
  8.1 Concern . . . . . . . . . . . . . . . . . . . . . . 7-21
  8.2 Purpose . . . . . . . . . . . . . . . . . . . . . . 7-21
  8.3 Approach . . . . . . . . . . . . . . . . . . . . . . 7-21
  8.4 Scope . . . . . . . . . . . . . . . . . . . . . . 7-23
    8.4.1 Procedure Review . . . . . . . . . . . . . . 7-24
    8.4.2 Organization Control . . . . . . . . . . . . 7-24
    8.4.3 Access Control . . . . . . . . . . . . . . . 7-25
    8.4.4 Contingency Plan . . . . . . . . . . . . . . 7-27

9. SECURITY FUNCTION REVIEW . . . . . . . . . . . . . . . . . . . 7-28
  9.1 Concern . . . . . . . . . . . . . . . . . . . . . . 7-28
  9.2 Purpose . . . . . . . . . . . . . . . . . . . . . . 7-28
  9.3 Approach . . . . . . . . . . . . . . . . . . . . . . 7-29
  9.4 Scope . . . . . . . . . . . . . . . . . . . . . . 7-29
  9.5 General . . . . . . . . . . . . . . . . . . . . . . 7-30
    9.5.1 Responsibility . . . . . . . . . . . . . . . 7-30
    9.5.2 Standard Operating Procedures/Users Manuals . . . . . . . . . . . . . . . . . 7-30
    9.5.3 Self-Reviews or Peer Reviews . . . . . . . . 7-30
    9.5.4 Education . . . . . . . . . . . . . . . . . 7-31
    9.5.5 Employee Awareness . . . . . . . . . . . . . 7-31
  9.6 Security Administration (Interactive Environment) . 7-31
  9.7 Access Control . . . . . . . . . . . . . . . . . . . 7-32
  9.8 Contingency Plan . . . . . . . . . . . . . . . . . . 7-32
  9.9 Summary . . . . . . . . . . . . . . . . . . . . . . 7-32

10. CONTROLLED TESTS/PENETRATION STUDY . . . . . . . . . . . . 7-32
  10.1 Concern . . . . . . . . . . . . . . . . . . . . . . 7-32
  10.2 Purpose . . . . . . . . . . . . . . . . . . . . . . 7-33
  10.3 Approach . . . . . . . . . . . . . . . . . . . . . . 7-33
  10.4 Scope . . . . . . . . . . . . . . . . . . . . . . 7-33
    10.4.1 Application Programming . . . . . . . . . 7-33
    10.4.2 Data Base/Data Communication Environment . . . . . . . . . . . . . . 7-34
    10.4.3 Information Security . . . . . . . . . . . 7-34
    10.4.4 Summary . . . . . . . . . . . . . . . . . 7-34

11. ISSUES FOR THE COMMUNITY . . . . . . . . . . . . . . . . 7-35
    11.1 Implications of Future Technology . . . . . . . . 7-35
    11.2 Adequacy of the Literature . . . . . . . . . . . 7-36
    11.3 State-of-the-Practice . . . . . . . . . . . . . . 7-37

REFERENCES . . . . . . . . . . . . . . . . . . . . . . . . 7-39

FIGURES
o Figure 1 Indicators of Application Sensitivity . . . . . 7-7
o Figure 2 System Levels of Security . . . . . . . . . . . 7-22

PART VIII: PROGRAM INTEGRITY . . . . . . . . . . . . . . . . 8-1
EDITORS' NOTE . . . . . . . . . . . . . . . . . . . . . . 8-2

Program Integrity Assessment . . . . . . . . . . . . . . . 8-3

1. WHAT IS PROGRAM INTEGRITY? . . . . . . . . . . . . . . 8-3

2. A CONTEXT FOR PROGRAM INTEGRITY . . . . . . . . . . . . 8-4
    2.1 Programs Change With Time (Life Cycle) . . . . . . 8-4
    2.2 Visibility of Relationships is Lost Between Stages . . . . . . . . . . . . . . . . . . . . . 8-5
    2.3 Program Integrity Assessment is Multi-Dimensional Problem . . . . . . . . . . . . . . . . . 8-6

3. RELEVANT THREATS AND THEIR SEVERITY . . . . . . . . . . 8-6

4. METHODS FOR ACHIEVING PROGRAM INTEGRITY . . . . . . . . 8-7
    4.1 Evidence of Correctness . . . . . . . . . . . . . 8-7
        4.1.1 Static Evaluation . . . . . . . . . . . . . 8-8
        4.1.2 Dynamic Evaluation . . . . . . . . . . . . 8-9
    4.2 Evidence of Robustness . . . . . . . . . . . . . 8-10
        4.2.1 On-Going Testing . . . . . . . . . . . . . 8-10
        4.2.2 On-Line Monitoring and Control . . . . . . 8-11
        4.2.3 Redundancy . . . . . . . . . . . . . . . . 8-11
        4.2.4 Support Control . . . . . . . . . . . . . 8-12
    4.3 Evidence of Trustworthiness . . . . . . . . . . . 8-12
        4.3.1 People . . . . . . . . . . . . . . . . . . 8-12
        4.3.2 Software Development . . . . . . . . . . . 8-13
        4.3.3 Tools . . . . . . . . . . . . . . . . . . 8-13

5. PROGRAM INTEGRITY IMPACTS OTHER SESSIONS . . . . . . . . 8-14

6. RECOMMENDATIONS . . . . . . . . . . . . . . . . . . . . 8-16
    6.1 Existing Software . . . . . . . . . . . . . . . . 8-16
    6.2 Future Software . . . . . . . . . . . . . . . . . 8-17
    6.3 Organization Actions . . . . . . . . . . . . . . 8-17

7. BIBLIOGRAPHY . . . . . . . . . . . . . . . . . . . . . 8-18

PART IX: DATA INTEGRITY . . . . . . . . . . . . . . . . . . . . 9-1
EDITORS' NOTE . . . . . . . . . . . . . . . . . . . . . . . . 9-2

Data Integrity Auditing: A Framework for Standards Development . . . . . . . . . . . . . . . . . . . . . . . . . 9-3

1. INTRODUCTION . . . . . . . . . . . . . . . . . . . . . . 9-3

2. DEFINITION OF DATA INTEGRITY . . . . . . . . . . . . . . . 9-4

3. OBJECTIVE OF DATA INTEGRITY AUDIT . . . . . . . . . . . . 9-4

4. SCOPE OF THE DATA INTEGRITY AUDIT . . . . . . . . . . . . 9-4
   o Reliability of the Data Source . . . . . . . . . . . . 9-5
   o Source Data Preparation . . . . . . . . . . . . . . . . 9-5
   o Data Entry Control . . . . . . . . . . . . . . . . . . 9-5
   o Data Input Acceptance Control . . . . . . . . . . . . . 9-6
   o Data Validation and Error Correction . . . . . . . . . 9-6
   o Processing Specification . . . . . . . . . . . . . . . 9-7
   o Output Controls and Distribution Procedures . . . . . . 9-7
   o Auditability . . . . . . . . . . . . . . . . . . . . . 9-7

5. APPROACH TO A DATA INTEGRITY AUDIT . . . . . . . . . . . . 9-8

6. METHODS FOR DATA INTEGRITY AUDITING . . . . . . . . . . . 9-9
   o Confirmation . . . . . . . . . . . . . . . . . . . . . 9-9
   o Sampling Techniques . . . . . . . . . . . . . . . . . . 9-9
   o Parallel Processing . . . . . . . . . . . . . . . . . . 9-10
   o Integrated Test Facility (ITF) . . . . . . . . . . . . 9-10
   o System Control Audit Review Files (SCARF) . . . . . . . 9-10
   o Tracing . . . . . . . . . . . . . . . . . . . . . . . . 9-10
   o Observation . . . . . . . . . . . . . . . . . . . . . . 9-10
   o Analysis by Interrogation of Existing Data . . . . . . 9-10
   o Test Decks or Test Data . . . . . . . . . . . . . . . . 9-10
   o Interviews . . . . . . . . . . . . . . . . . . . . . . 9-11
   o Program Source Code Review . . . . . . . . . . . . . . 9-11
   o Questionnaires . . . . . . . . . . . . . . . . . . . . 9-11
   o Code Analysis and Mapping . . . . . . . . . . . . . . . 9-11
   o Automatic Flowcharting Software . . . . . . . . . . . . 9-11
   o Procedural Walk-throughs . . . . . . . . . . . . . . . 9-11
   o Undercover Observations . . . . . . . . . . . . . . . . 9-12
   o Surprise Visits . . . . . . . . . . . . . . . . . . . . 9-12
   o Analysis of System Activity Logs . . . . . . . . . . . 9-12
   o Continuous Monitoring and Surveillance Software . . . . 9-12

PART X: COMMUNICATIONS . . . . . 10-1
EDITORS' NOTE . . . . . 10-2

Audit and Control of Data Communications Networks . . . . . 10-3

1. INTRODUCTION . . . . . 10-3
  o Definition of the Special Data Communication Audit . 10-3
  o The Exposures . . . . . 10-3
  o How to Audit a Data Communications Network . . . . . 10-4
  o Limitations . . . . . 10-6

2. USE OF THE AUDIT MATRIX . . . . . 10-9

3. DEFINITION OF RESOURCES, EXPOSURES AND SAFEGUARDS . . . 10-10
  o Resources . . . . . 10-10
  o Exposures . . . . . 10-11
  o Safeguards . . . . . 10-12

Figure 1 End to End Communication Network . . . . . 10-5
Table 1 Matrix of Safeguards to Audit a Data Communications Network . . . . . 10-7, 10-8

PART XI: POST-PROCESSING AUDIT TOOLS AND TECHNIQUES . . . . . 11-1
EDITORS' NOTE . . . . . 11-2

Post-Processing Audit Tools and Techniques . . . . . 11-3

1. INTRODUCTION . . . . . 11-3

2. OBJECTIVES OF A TYPICAL SECURITY AUDIT . . . . . 11-3

3. DEFINITIONS . . . . . 11-4

4. SCOPE OF POST-PROCESSING AUDIT . . . . . 11-5

5. INFORMATION REQUIREMENTS . . . . . 11-5

6. TYPICALLY AVAILABLE INFORMATION . . . . . 11-10

7. ILLUSTRATIVE EXAMPLE: ELECTRONIC FUNDS TRANSFER SYSTEM . . . . . 11-11
  7.1 Remote Terminal Procedures . . . . . 11-11
  7.2 Message Security at the Switching Computer . . . . 11-11
    7.2.1 Message Headers . . . . . 11-11
    7.2.2 Message Acknowledgement and Release . . . . 11-13
    7.2.3 Ledger Balancing . . . . . 11-13
  7.3 Communications Processor Logs . . . . . 11-13
  7.4 Bank Computer Functions and Logs . . . . . 11-13

8. POST PROCESSING TECHNIQUES . . . . . . . . . . . . . . . . . 11-13
  8.1 ACCESS . . . . . . . . . . . . . . . . . . . . . . . . . 11-13
    8.1.1 Unsuccessful Accesses . . . . . . . . . . . 11-13
    8.1.2 Successful Accesses . . . . . . . . . . . . 11-17
    8.1.3 Log Continuity Check . . . . . . . . . . . . 11-17
  8.2 INPUT . . . . . . . . . . . . . . . . . . . . . . . . . 11-17
  8.3 PROCESSING . . . . . . . . . . . . . . . . . . . . . . 11-17
    8.3.1 Manual Checking . . . . . . . . . . . . . . 11-17
    8.3.2 Control Totals . . . . . . . . . . . . . . . 11-17
    8.3.3 Test Data . . . . . . . . . . . . . . . . . 11-17
    8.3.4 Integrated Test Facility . . . . . . . . . . 11-17
    8.3.5 Tagging . . . . . . . . . . . . . . . . . . 11-17
    8.3.6 Extended Record Maintenance . . . . . . . . 11-17
    8.3.7 Tracing . . . . . . . . . . . . . . . . . . 11-18
    8.3.8 Mapping . . . . . . . . . . . . . . . . . . 11-18
    8.3.9 Recompilation . . . . . . . . . . . . . . . 11-19
    8.3.10 Parallel Simulation . . . . . . . . . . . . 11-19
    8.3.11 Retrieval Programs . . . . . . . . . . . . 11-19
  8.4 OUTPUT . . . . . . . . . . . . . . . . . . . . . . . . 11-19
    8.4.1 Output Listing . . . . . . . . . . . . . . . 11-19
    8.4.2 Authorization Listing . . . . . . . . . . . 11-19

9. NEEDED TECHNIQUES . . . . . . . . . . . . . . . . . . . . 11-20
  9.1 Logging Methods . . . . . . . . . . . . . . . . . . . 11-20
  9.2 Software Tools . . . . . . . . . . . . . . . . . . . . 11-20

10. CONCLUSIONS AND RECOMMENDATIONS . . . . . . . . . . . . . 11-21

11. REFERENCES . . . . . . . . . . . . . . . . . . . . . . . 11-21

FIGURES

o Figure 1 Post Processing Security Audit . . . . . . . . . 11-6
o Figure 2 Security Considerations Within EFTS System Architecture . . . . . . . . . . . . . . . . . . . 11-12
o Figure 3 Techniques in Support of Audit Objectives . . . 11-19

TABLES

o Table 1 System Log Access Information . . . . . . . . . 11-7
o Table 2 Input Log Information . . . . . . . . . . . . . 11-8
o Table 3 Processing Log Information . . . . . . . . . . . 11-8
o Table 4 Output Log Information . . . . . . . . . . . . . 11-9
o Table 5 Operating System--Security Access Control Log Data . . . . . . . . . . . . . . . . . . . . . 11-14
o Table 6 Security Requirements During Edit/Validation of Input Transactions . . . . . . . . . . . . . . 11-15
o Table 7 Security Requirements During Processing/Update of Data . . . . . . . . . . . . . . . . . . . . . 11-15
o Table 8 Security Requirements During Output of Data . . 11-15

PART XII: INTERACTIVE AUDIT TOOLS AND TECHNIQUES . . . . . . . . . 12-1
EDITORS' NOTE . . . . . . . . . . . . . . . . . . . . . . . . . 12-2

Interactive Audit Tools and Techniques . . . . . . . . . . . . 12-2

1. EXECUTIVE SUMMARY . . . . . . . . . . . . . . . . . . . . . 12-3
    1.1 Introduction . . . . . . . . . . . . . . . . . . . . . 12-3
        1.1.1 Interactiveness . . . . . . . . . . . . . . . . . 12-3
        1.1.2 Research and Development . . . . . . . . . . . . 12-3
        1.1.3 Subject Areas . . . . . . . . . . . . . . . . . . 12-3
    1.2 Summary . . . . . . . . . . . . . . . . . . . . . . . . 12-3
        1.2.1 Performance Assurance . . . . . . . . . . . . . . 12-3
        1.2.2 Existing Tools and Techniques . . . . . . . . . . 12-4
        1.2.3 Needed Tools and Techniques . . . . . . . . . . . 12-4
    1.3 Use of Interactive Tools and Techniques . . . . . . . . 12-4
    1.4 Benefits of Interactive Tools and Techniques . . . . . 12-5
    1.5 Further Deliberation and Research . . . . . . . . . . . 12-5

2. GOAL, OBJECTIVES, DEFINITIONS . . . . . . . . . . . . . . . 12-6
    2.1 Goal . . . . . . . . . . . . . . . . . . . . . . . . . 12-6
    2.2 Objectives . . . . . . . . . . . . . . . . . . . . . . 12-6
    2.3 Definitions . . . . . . . . . . . . . . . . . . . . . . 12-6
        2.3.1 Performance Assurance . . . . . . . . . . . . . . 12-6
        2.3.2 Interactive Tools and Techniques . . . . . . . . 12-6
        2.3.3 Interactive Audit Programming . . . . . . . . . . 12-6
        2.3.4 Interactive Audit Processing . . . . . . . . . . 12-8
        2.3.5 Interactive Auditing . . . . . . . . . . . . . . 12-8
        2.3.6 On-Line Auditing . . . . . . . . . . . . . . . . 12-8
        2.3.7 Auditing of On-Line Systems . . . . . . . . . . . 12-8
    2.4 Performance Assurance Functions . . . . . . . . . . . . 12-8
        2.4.1 Model . . . . . . . . . . . . . . . . . . . . . . 12-8
        2.4.2 CPA Functions . . . . . . . . . . . . . . . . . . 12-9
        2.4.3 Internal Auditor Functions . . . . . . . . . . . 12-9
        2.4.4 Quality Assurance Functions . . . . . . . . . . . 12-9
        2.4.5 Operating and Line Management Functions . . . . 12-9

3. PERFORMANCE ASSURANCE ACTIVITIES . . . . . . . . . . . . . 12-9
    3.1 Introduction . . . . . . . . . . . . . . . . . . . . . 12-9
    3.2 Setting PA Objectives . . . . . . . . . . . . . . . . . 12-10
    3.3 Gathering Information . . . . . . . . . . . . . . . . . 12-10
    3.4 Performing PA Analyses and Evaluations . . . . . . . . 12-10
    3.5 Designing and Performing PA Test Procedures . . . . . 12-11
        3.5.1 Select the Verification Techniques . . . . . . . 12-11
        3.5.2 Determine if Computer Assisted Techniques Will be Used . . . . . . . . . . . 12-12
        3.5.3 Prepare and Perform Test Procedures . . . . . . 12-12
        3.5.4 Review Test Results and Determine if Further Tests are Required . . . . . . . . . 12-12

4. EXISTING PERFORMANCE ASSURANCE TOOLS AND TECHNIQUES . . 12-12
  4.1 Introduction . . . . . . . . . . . . . . . . . . . . . . 12-12
  4.2 Batch PA Tools and Techniques . . . . . . . . . . . . 12-13
    4.2.1 Utility Programs . . . . . . . . . . . . . . . . 12-13
    4.2.2 Test Decks . . . . . . . . . . . . . . . . . . . 12-13
    4.2.3 Audit Modules . . . . . . . . . . . . . . . . . . 12-13
    4.2.4 ITF (Integrated Test Facility) . . . . . . . . 12-14
    4.2.5 Test Data Generator . . . . . . . . . . . . . . 12-14
    4.2.6 Snapshot . . . . . . . . . . . . . . . . . . . . 12-14
    4.2.7 Tracing . . . . . . . . . . . . . . . . . . . . . 12-14
    4.2.8 SCARF (System Control Audit Review File) . . 12-15
    4.2.9 Audit Software Packages . . . . . . . . . . . . 12-15
    4.2.10 Parallel Simulation . . . . . . . . . . . . . . 12-15
  4.3 Interactive PA Tools and Techniques . . . . . . . . . 12-16
    4.3.1 ACL (Audit Command Language) . . . . . . . . . 12-16
    4.3.2 NAARS (National Automated Research System) . . . . . . . . . . . . . . . . . . 12-16

5. NEEDED PERFORMANCE ASSURANCE TOOLS AND TECHNIQUES . . . 12-16
  5.1 Introduction . . . . . . . . . . . . . . . . . . . . . . 12-16
  5.2 Needed Tools and Techniques . . . . . . . . . . . . . 12-17
    5.2.1 Near Real-Time Error Detection and Correction . . . . . . . . . . . . . . . . . . . 12-17
    5.2.2 Monitoring of Adequacy of Controls . . . . . 12-17
    5.2.3 Measurement of Design Accuracy . . . . . . . . 12-18
    5.2.4 Program Modification Control . . . . . . . . . 12-18
    5.2.5 Monitoring System Trouble Indicators . . . . 12-18

6. SUMMARY AND RECOMMENDED FOLLOWUP . . . . . . . . . . . . . 12-20
  6.1 Introduction . . . . . . . . . . . . . . . . . . . . . . 12-20
  6.2 Need for Interactive Tools and Techniques . . . . . 12-20
  6.3 Recommended Followup . . . . . . . . . . . . . . . . . 12-21
    6.3.1 Design Criteria . . . . . . . . . . . . . . . . 12-21
    6.3.2 Interfaces . . . . . . . . . . . . . . . . . . . 12-21
    6.3.3 Behavioral Research . . . . . . . . . . . . . . 12-21
    6.3.4 Theory . . . . . . . . . . . . . . . . . . . . . 12-22

REFERENCES . . . . . . . . . . . . . . . . . . . . . . . . . 12-22

FIGURES

o Figure 1 Interactive Auditing . . . . . . . . . . . . . 12-7
o Figure 2 Performance Assurance . . . . . . . . . . . . 12-8
o Figure 3 PA Tools and Techniques by PA Functions . . . . 12-19
o Figure 4 Needed Performance Assurance Tools and Techniques . . . . . . . . . . . . . . . . . 12-20

APPENDIX A: WORKSHOP ATTENDEE LIST . . . . . . . . . . . . . A-1

APPENDIX B: EVOLUTION OF THE WORKSHOP AND PROCEEDINGS ...... B-1

1. INITIATING THE WORKSHOP .................. B-1
2. PLANNING THE WORKSHOP .................. B-1
    2.1 Workshop Format .................. B-2
    2.2 Workshop Topics and Chairmen .................. B-2
    2.3 Pre-Workshop Session Activities .................. B-3
3. AT THE WORKSHOP .................. B-3
4. THE SESSION REPORTS .................. B-4

# EXECUTIVE SUMMARY

On March 22-24, 1977 an Invitational Workshop on Audit and Evaluation of Computer Security was held by the National Bureau of Standards (NBS) in Miami Beach, Florida. The Workshop was planned and carried out by NBS with the support of the U.S. General Accounting Office (GAO). This Workshop is the first part of a two phase effort, originating within Task Group 15 (TG-15) of the Federal Information Processing Standards (FIPS) Program, in the Computer Security Audit area. The goals of the Workshop were to consolidate the state-of-the-art information available in the field and to define areas for future research. The goal of the second phase of this effort will be to adapt this information to the needs of Federal agencies in the form of Federal Information Processing Guidelines. It is expected that this latter task will be carried out by a working group convened for this purpose.

Under the direction of Robert G. McKenzie of the U.S. General Accounting Office and with Zella G. Ruthberg as the National Bureau of Standards liaison, an informal task team within TG-15 planned the Workshop format and subject matter. The result was a relatively small invitational topic area workshop to cover ten non-mutually exclusive major areas of concern in computer security audit.

With inputs from the task team as well as the Institute of Internal Auditors, the American Institute of Certified Public Accountants, and the Canadian Institute of Chartered Accountants, an outstanding group of session Chairmen, Recorders, and attendees drawn from the audit and computer communities was selected. The three days at the Workshop allowed these people to develop the basis for the ten reports contained in these Proceedings. The following material summarizes these ten reports. The reports are independent of one another and may be read in any order. Note that the reports toward the beginning of the Proceedings are more management oriented and the later ones more technically oriented.

## SESSION ON INTERNAL AUDIT STANDARDS

In response to their charge to develop a proposed statement of audit standards for computer security , this group first defines the larger subject of internal audit of a computer system, and then defines computer security audit. It characterizes this audit as covering accountability, primarily in the areas of compliance and program results. It concludes that the GAO pamphlet entitled "Standards for Audit of Governmental Organizations, Programs, Activities and Functions" forms a sound foundation for internal audit standards for EDP audit and that all that is needed are supplemental standards such as AICPA's SAS3 to define additional tasks that the auditor must perform in a computer security audit to meet these basic standards. Three areas are identified for these supplemental standards:

1. Systems Development,
2. Operational Systems (Applications Controls), and
3. Physical Security and General Controls.

In the area of Systems Development, audit involvement would assure that plans are made for controls against theft and error, appropriate audit trails, conformity with management objectives and with the law, sufficient documentation, appropriate design approval mechanisms, and general efficiency and economy. In the area of Operational Systems, audit would check that the application conforms to standards and the latest design specifications, and that the internal controls and reliability of data are sound. In the Physical Security and General Controls area, audit would verify that the organization structure, the physical facilities, the personnel management, the back-up capability, and the software/hardware controls all help meet management's objectives.

The recommendations for action by this session were:

1. that GAO review these supplementary standards and consider adding them to their other standards;
2. that these supplementary standards be reviewed and endorsed by the Federal Audit Executive Council; and
3. that NBS consider these supplemental standards for inclusion in a FIPS guideline in the area of audit for computer security.

## SESSION ON QUALIFICATIONS AND TRAINING

In response to the question, "What are the qualifications and training necessary to conduct audit of computer security?," this group draws up an outline of the broad body of knowledge needed to perform a computer security audit. Some of the considerations that shape their reply are that

1) computer security involves all controls needed to ensure the integrity, accuracy, and reliability of the acquisition, processing, storing, and dissemination of information;
2) persons performing this audit should have an initial degree in (but not limited to) such disciplines as accounting, business administration, engineering, operations research, computer science, or economics plus a solid supplementary foundation in management, auditing, data processing, and/or telecommunications;
3) audit of more complex systems require so many of these disciplines that an interdisciplinary team should probably be used;
4) training is available or can be installed in all the standard educational channels;
5) costs cannot be estimated because there are too many variables in going from one organization to the next; and

6) there are at least three levels of knowledge needed for the work:
    a) general management and auditing concepts,
    b) data processing and telecommunications expertise, and
    c) a comprehensive integration of the first two obtained through further training and experience.

The broad categories in the outline of the common body of knowledge are:

1. Computer systems, operations, and software;
2. Data processing techniques;
3. Management of the data processing function;
4. Security of the data processing function;
5. Risk analysis and threat assessment;
6. Management concepts and practices;
7. Auditing concepts and practices;
8. Additional qualifications needed to evaluate computer security.

A brief discussion of each of these categories is given. The final outline contains a listing of the major disciplines appropriate for each category.

## SESSION ON SECURITY ADMINISTRATION

This session responded to the question, "What audit approaches and techniques can be used in an evaluation of the security administration function?" Initially this group discusses the legal basis for establishing a Security Administration Function in a Federal organization--the Brooks Act (PL-89-306) and the Privacy Act of 1974. It also proposes that the Security Administration Function must be defined in detail so that audit of that function becomes a standard compliance type review. The bulk of the rest of the paper is devoted to defining the Security Administration Function.

An important related issue, mentioned in the early part of the paper concerns the need for international privacy law compatibility. Privacy legislation has already been passed in Sweden and Germany and is pending in Norway, Denmark, and France. International organizations will be finding this an important issue in the years to come. The report has an Appendix outlining the German privacy law.

Some of the important points made about the Security Administration Function are that

1. Responsibility for safeguarding an organization's data and information resources belongs to those individuals having physical custody and accountability for it, i.e. all levels of line management.
2. The Security Administration Program is a staff function and should consist of developing overall policy and monitoring overall effectiveness.
3. Planning for security administration should be carried out at

three management levels:

a) broad policy level using top management input,
b) an intermediate policy level developing implementation instructions,
c) the implementation level developing schedules and resource requirements.

4. Management controls to ensure that security objectives are achieved fit into three categories-- policies that are formulated at the top, procedures for administrative, physical, and technical security measures, and practices for the standard management activities.
5. ADP security controls should include a) administrative safeguards in the form of contingency plans, security documentation, authorization control lists, program access controls, personnel rules; b) physical security safeguards such as area restrictions, disaster back-up, storage libraries, disposal procedures; and c) technical security in the form of a security system to handle data and files, program libraries, operating system(s), teleprocessing, and encryption.
6. Training is needed for systems people as well as users.

An example of a suggested security system for an on-line system is then given.

The final requirements of the group are that the Audit and Security Administration functions should be independent of one another and that the Audit function reports to the agency head. Given this set of conditions and the clear definition of the Security Administration function, the audit of this function is then a compliance review.

## SESSION ON AUDIT CONSIDERATIONS IN VARIOUS SYSTEM ENVIRONMENTS

The question this session considered was, "What are the considerations to be given to the audit of computer security in various system environments?" This group identifies four conceptual modules for the development of an open-ended structured model of computer security audit. These are:

1. Defining three vital audit components--access control, accuracy, and availability.
2. Describing a morphology of systems and environments: Physical components, systems structure, and people. The systems are described by five identifiable characteristics --number of users, types of service, system organization, user access, and application mix.
3. Defining a methodology-- a computer audit model-- which establishes a scorecard value for each parameter capable of being audited.
4. Performing a model validation by testing the model with four examples.

This group declares that an auditor goes through a set of steps parallel to those executed by a design team. It then proceeds to outline the design team activity, i.e. to define requirements, objectives, and sensitivity; to specify the physical, system, and administrative parameters; to specify possible control techniques; to make four judgements concerning each control--

1. cost,
2. effectiveness in maintaining access control,
3. effectiveness in maintaining accuracy,
4. effectiveness in maintaining availability,

giving each of the three effectiveness aspects of the control a theoretical score of 1 to 10 and using all four to make decisions on whether or not to use the control. The next design team activities then are to select a subset of these controls to provide the desired level of protection; to incorporate these controls into the environment, to reassess the system, and to iterate until all requirements are satisfied. The parallel operations performed by an auditor would be: to review the objectives, requirements, and sensitivity; to determine the actual environment; to identify the control techniques being used; to perform a cost and effectiveness analysis, this time using hardware and software techniques to give each control its composite score; and to prepare a report on the findings. The group developed a tabulation sheet for recording these findings for any particular system. The paper has four system examples on the tabulation sheets to illustrate this approach to computer security. It also points out that there are currently no standard methods for evaluating a control, i.e. giving it a score of 1 to 10. This is the area that needs a considerable amount of future effort.

## SESSION ON ADMINISTRATIVE AND PHYSICAL CONTROLS

This group responded to the question, "What are the audit approaches and techniques for evaluation of administrative and physical controls in an ADP environment, including contingency planning, etc.?" The group initially establishes the thesis that the concerns of data security and the responsibilities of the auditor are complementary since both deal with the protection of resources within the data processing mission. The areas of concern to the auditor all have problems associated with them. Some of the more important areas mentioned are

1. the need for a workable definition of security
2. the need for an explicit statement of security policy
3. the need for accepted standards of good practice
4. the need to know what tests and examinations are appropriate
5. the need to know the hazards that a system is subject to.

The remainder of the report covers suggestions for the auditor.

First, four general areas of interest to the auditor are discussed and then five non-mutually exclusive audit approaches to data processing security are discussed in detail. The four general areas are

1. Audit focus and materiality--Security protective measures should

yield "an acceptable level of risk." The auditor should review that this is the case, particularly for the most sensitive applications.

2. Standards of practice and their documentation--Five references are briefly discussed for their contributions in this area. The best single one is stated to be "Computer Control Guidelines" and "Computer Audit Guidelines" by the Canadian Institute of Chartered Accountants.
3. Security audit report--An outline of a security audit report is given in two parts- one part addressed to higher management and the second to the auditee and his management.
4. Best traditional audit techniques--These are:
    Selective protection--review key resource protection,
    Test--use actual tests where possible,
    Interview--with all involved employees and management,
    Technical cooperatives (co-op)--use talent from other organizations and locations.

The five audit approaches are each discussed under the headings Concern, Purpose, Approach, and Scope. They are:

1. System Development and Maintenance Practices Audit
2. Application Review
3. Installation Security Review
4. Security Function (Data Base/Communication Environment) Review
5. Compromise Attempt.

The report concludes that the issues for the DP community lie in adapting to the new technologies (increasing portability of storage media, mass storage, and distributed systems), satisfying the need for a single compendium of audit concerns and techniques, and improvement and change by management in programming application development and system development.

## SESSION ON PROGRAM INTEGRITY

This session responded to the question "What are the audit approaches and techniques for evaluation of program integrity in an ADP environment?" It emphasizes that program integrity must be considered over the entire life cycle of the program. Program integrity concerns: 1) correctness in fulfilling requirements and doing nothing else; 2) satisfaction of trained user expectations; 3) usefulness in fulfilling an intended mission; and 4) the ability to be evaluated so that a level of trust in the program can be established.

Program integrity assessment is a multi-dimension problem. Determining when in the life cycle to audit is one dimension. Other dimensions include the severity of the security threat and the methods employed during development to achieve integrity.

The methods for achieving program integrity can be put into three categories:

1. those that give evidence the program is correct,
2. those that show it is robust and will perform adequately in the face of unexpected events,
3. those that show it is trustworthy and developed in accord with good practice.

A discussion of methods in each of these categories is included in the paper.

The recommendations from the group are:

For existing sotware:

1. Be cautious in assuming program integrity exists.
2. Use the limited existing tools, guided by a careful risk management analysis.
3. Improve physical and administrative controls and thus reduce the effect of lack of program integrity.
4. Reduce the exploiter population by access controls.
5. Reduce asset exposure by removing assets from the system when they are not in use.

For future software:

1. Improve the program production process.
2. Assure program integrity compliance through the entire life cycle.

For organizations:

1. Perform a self-assessment of its threats and its involvement in the life cycle of the programs it uses.
2. Create guidelines for the development and acquisition of software that is auditable for program integrity.

## SESSION ON DATA INTEGRITY

The question addressed by this group was, "What are the audit approaches and techniques for evaluation of the data integrity in an ADP environment?" The group decided to limit itself to considerations of those safeguards having a direct bearing on data integrity audit, assuming that physical, operational, administrative, and software measures--all necessary for data integrity--would be handled by other sessions. This group defined data integrity as the state that exists when data is (within defined limits of reliability) accurate, consistent, authorized, valid, complete, unambiguaous, and processed according to specifications in a timely manner. The objectives of a data integrity audit are evaluation of compliance with and adequacy of existing policies and procedures, and recommendations of corrective actions.

To achieve this objective, one needs to evaluate the following areas:

- o reliability of the data source
- o source data preparation
- o data entry controls
- o data input acceptance controls
- o data validation and error correction
- o processing specifications
- o output and distribution controls

and

- o auditability.

The group then outlined activities for producing a comprehensive audit work plan, and briefly discussed a variety of methods for data integrity auditing. Some of those included are:

- o checks with users on accuracy, completeness, and consistency;
- o possible sampling techniques;
- o parallel processing;
- o integrated test facility (ITF);
- o System Control Test Review File (SCARF);
- o tracing tagged transactions;
- o test decks;
- o questionnaires;
- o procedural walk-throughs;
- o activity logs.

## SESSION ON COMMUNICATIONS

This group responded to the question, "What are the audit approaches and techniques for evaluation of communications in an ADP environment?" They limit their discussion to guidelines for a data communication security audit of a computer system that uses a data communication network. This audit applies to the hardware, software, and people involved with the data communications of the computer system. The group recommends that such an audit should be made on sensitive applications and the general data communications system, with the frequency being directly related to the sensitivity of the applications or system. The general approach for this type of audit should be a transaction flow analysis, tracking transactions both from the input terminal through the network to the computer, and in the reverse direction (computer to terminal).

A specific tool developed by the group for conducting this type audit is a resource/exposure/safeguard matrix. This matrix contains a list of ten system resources down the left hand side, a list of six categories of exposure across the top and an enumeration of appropriate safeguards that might be in place for each combination of resources and exposures. The auditor's job would then be to determine what are the actual resources of the computer system (terminals, distributed intelligence, modems, local loops, lines, multiplexors/concentrators/switches, front-end processor, computer, software, and people); and to see what safeguards are in place to protect these resources against the possible exposures (errors and omissions, disaster and disruptions, loss of integrity, disclosure, defalcation, and theft of resources). Each of the seventeen safeguards in the report (as well as the resources and exposures) are defined. In addition, for each safeguard there is a statement about what the auditor should do with respect to his review of this safeguard.

The paper points out its own limitations--that the safeguards are not all-inclusive, will only assist in achieving security but not guarantee it, may not apply to all applications, and only reflect the current state-of-the-art methods.

## SESSION ON POST-PROCESSING AUDIT TOOLS AND TECHNIQUES

The question this group addressed was, "What are the post-processing audit tools and techniques available or needed for the effective use of the various system journals and logs in an audit of computer security?" They initially describe the general objectives of such an audit as determining the existence, scope, and adequacy of controls in the light of level of protection required. They note the specific objectives as establishing the existence of uniqueness of transactions, transaction integrity (completeness, accuracy, and authorization controls), processing integrity, distribution controls, recoverability controls, and violation controls. The terms "computer security", "computer security audit", "post-processing audit", "logs", "tools vs. techniques", and "transaction" are defined to enhance the clarity of the document.

This group then describes what it considers to be the essence of a post-processing security audit. Such an audit is always concerned with

- o INPUT
- o PROCESS
- o OUTPUT

and

- o ACCESS to any of the above three.

The objectives of a security audit can be achieved by looking for information detailed in a log on any of the above components. This log would show five basic types of information:

1. WHO--identifies initiator of an action,
2. FUNCTION--describes the processing activity,
3. WHAT--identifies objects of processing activity,
4. STATUS--refers to FUNCTION and associated initiator and affected objects,
5. TIME--gives it a date-time stamp.

An example is given of the security information requirements for an EFTS system.

Post-processing techniques are then described under the basic four components of an audit. For Access and Input one would use logs of successes, logs of failures, and a log continuity check. For Process there are manual checking, control totals, test data, integrated test facility, tagging, extended record maintenance, tracing, mapping, recompilation, parallel simulation, and retrieval programs. For Output there are output listings of dispositions and authorization listings.

The conclusions and recommendations of the group were:

1. Existing software tools offer much but could be made easier to use by
    a) publishing a catalog of these tools for the auditor.
    b) creating facilities to easily combine the use of two of these tools.
2. Needed techniques are
    a) a method for maintaining the security of the security log. (Some possibilities are using present operating systems, or using a special tamper proof recording device to record all activity, or a complete hardware monitor similar to a cockpit flight recorder).
    b) higher level software to access and manipulate logs.

## SESSION ON INTERACTIVE AUDIT TOOLS AND TECHNIQUES

This group responded to the question, "What are the interactive audit tools and techniques available or needed to permit on-line auditing of computer security?" This session explored a subject area which is in the very early stages of development. The group defines its overall goal as "The development of an auditing approach for the use of on-line or interactive techniques to achieve performance assurance in computer systems." and its specific objectives as

1. Define the scope and requirements for interactive tools and techniques.
2. Review and define auditability and control characteristics in computer systems.
3. Describe tools and techniques available and specify needed ones.
4. Develop criteria for the use of these tools in specific systems environments and define the required interfaces (e.g. with Data Base, Operating Systems).

In order to achieve these objectives the group first defines a number of terms, the most central one being 'interactive auditing'-an activity consisting of interactive audit programming and interactive audit processing. Interactive audit for computer security is then put into the larger framework of Performance Assurance (PA) (defined as assuring that a computer system is performing its intended functions within a specified degree of accuracy, timeliness, and data security, and that it is not performing unintended functions). Performance assurance is initially described in terms of the functions performed by several different kinds of people, including the Certified Public Accountant, senior organizational management, internal auditors, the quality assurance function, and operational management. However, the PA function is largely discussed in terms of four activities:

1. Setting PA objectives relating to
    a) the nature and purpose of the testing,
    b) the nature of the computer system being tested;
2. Gathering information needed to review, evaluate, or establish systems, procedures, and controls;
3. Performing PA analyses and evaluations suitable for the nature and complexity of the system application;
4. Designing and performing PA test procedures as a result of the analyses and evaluations.

Existing audit tools and techniques to accomplish the above PA activities are divided into two classes, batch and interactive, with advantages and disadvantages of each being given. Available batch tools are utility programs, test decks, audit modules, integrated test facility (ITF), test data generator, snapshot (with tagging), tracing, SCARF, audit software packages, and parallel simulation. Interactive tools are Audit Command Language (ACL) and National Automated Accounting Research System (NAARS). The benefits of interactive tools and techniques are discussed. All audit tools and techniques are tabulated by PA activities performed.

A comprehensive discussion of needed tools and techniques is then given. They are divided into five broad categories:

1. near real-time error detection and correction,
2. monitoring of adequacy of controls,
3. measurement of design accuracy,
4. program modification control,
and
5. monitoring system trouble indicators.

This part of the report outlines a large number of tools that need development in order to make interactive auditing a reality. These tools and techniques are also tabulated by PA activities performed.

The broad recommendations of this group are that further deliberations and research are required in the following areas:

1. Specifications of design and performance requirements for interactive audit tools and techniques.
2. Designs of interactive audit tools and techniques for interfaces with operating systems and data base management systems.
3. Behavioral audit research to study audit behavior in an interactive human-machine mode of operation.
4. Development of a comprehensive audit and control theory to guide PA professionals in their activities and software designers in the development of appropiate audit tools and techniques.

# PART I: INTRODUCTION

## 1. HOST WELCOMING ADDRESS

S. Jeffery
National Bureau of Standards

I'd like to welcome all of you to the National Bureau of Standards' Invitational Workshop on Audit and Evaluation of Computer Security. This will be a memorable meeting because of the qualifications of those here today, as well as the broad scope of organizations and disciplines they represent.

It is interesting to note that 33% of the Workshop attendees represent nearly a dozen Federal agencies and organizations. The Federal agencies include: the General Accounting Office, the Department of Health, Education, and Welfare, the Department of Defense, the General Services Administration, the Department of Agriculture and, of course, our own Department of Commerce.

Although we have an impressive list of persons from these various Government agencies, I would especially like to welcome Frank S. Sato, the Deputy Assistant Secretary of Defense for Audit; Donald L. Scantlebury, the Director of the Financial and General Management Studies Division of the General Accounting Office; Howard R. Davia, the Director of the Office of Audit at the General Services Administration; Donald L. Eirich, Associate Director of the Logistics and Communications Division of the General Accounting Office; and C. William Getz, Regional Commissioner of the General Services Administration, Region 9.

Their respective experience will provide an important addition to the rich mixture of knowledge here today.

The remaining 67% of the attendees come from accounting firms, software and hardware organizations, private industry, and universities.

We have a solid contingent from the accounting world with six firms represented. There are seven software houses and two main-frame manufacturers; in the university area, three U.S. universities; and in the private sector, twenty-two firms drawn from such diverse fields as banking, utilities, the fuel industry, insurance, research, publishing, a credit bureau, the photographic industry, and law enforcement--as represented by the Royal Canadian Mounted Police.

A second cut at the attendee list for this Workshop can be made from the point of view of skills and knowledge represented. The audit aspect of this Workshop is covered by persons from the American Institute of Certified Public Accountants, the Institute of Internal Auditors, the EDP Auditors Association, the Association of Government Accountants, six large accounting firms in the private sector, and auditors from various Government and private organizations.

The computer aspect of our Workshop is represented by persons engaged in developing control software and techniques for industry, for Government, and for universities with a strong contingent of leading-edge researchers in all these areas.

It should be clear from all that I have said that we have an unusual array of talents assembled for this workshop.

I think that this is the first time that such a breadth and depth of abilities has been focused on the subject of audit and evaluation of computer security.

I'd like to thank our Chairman, Mr. Robert G. McKenzie of the General Accounting Office for his efforts in guiding the evolution of this Workshop. He was instrumental in selecting the topics for discussion in the various sessions and Session Chairmen, and provided constant guidance in the selection of session attendees.

My thanks also to Mrs. Zella G. Ruthberg of my own staff who has worked with Bob McKenzie throughout the planning. She has also been responsible for coordinating all arrangements for finding and obtaining these fine accommodations.

Our specific interest in this Workshop is to accumulate sufficient information to form the basis for Federal Information Processing Standards and Guidelines in the area of audit and evaluation of computer security.

The Institute for Computer Sciences and Technology of the National Bureau of Standards has the responsibility of providing Federal agencies with standards and guidelines for data processing, and it is expected that the Proceedings of this Workshop will be the precursor to such a guideline.

Considering the broad spectrum of abilities assembled here, these Proceedings will undoubtedly be a valuable document in itself, to be used by all those working in the internal audit areas.

Again, let me thank you all for your interest in coming, and I want to wish you every success in your efforts.

## 2. EDITOR'S COMMENTS ON THE SESSIONS AND THE REPORTS

### 2.1 Some Definitions of Terms

Each attendee was furnished a copy of FIPS PUB 39, "Glossary for Computer System Security," in an attempt to maintain uniformity of technical terms in the reports of the various sessions. A number of the sessions chose to redefine a few terms and use others not included in the Glossary. In most of these cases, the definitions as used by the session participants have been included as an integral part of their reports. The following is a discussion of a few terms considered to be essential.

Computer security audit. An independent evaluation to determine (1) the accuracy and reliability of the data maintained on or generated by an automated data processing system, (2) the adequacy of protection afforded the organization's assets to include hardware, software, and data from all significant anticipated threats or hazards, and (3) the operational reliability and performance assurance of the automated data processing system.

Internal audit. An independent appraisal activity within an organization for the review of operations as a service to management. The overall objective of internal auditing is to assist management in attaining its goals by furnishing information, analyses, appraisals, and recommendations pertinent to management's duties and objectives. The need for effective internal auditing in the Federal agencies has been recognized by the Congress in a number of laws, particularly the Budget and Accounting Procedures Act of 1950 which requires the head of each agency to establish and maintain

> "... internal control designed to provide...
> effective control over and accountability for all funds,
> property, and other assets for which the agency is
> responsible, including appropriate internal audit."

External audit. Frequently considered synonymous with financial audits conducted by certified public accountants. Financial audits are objective examinations of financial statements, accompanied by the expression of a competent opinion concerning the fairness of the presentation of those financial statements. However, a broad definition of external audit would simply be: An audit of any type conducted by individuals independent of the organization under review.

## 2.2 Observations

Audit and evaluation of computer security is a very complex subject that must be considered from a total system perspective. It involves the evaluation of all of the controls necessary to assure computer security as defined under "computer security audit" in section 2.1.

The total security system that provides such assurance consists of controls that can be grouped into various categories, such as physical, procedural, operational, technical, etc. However, it does little good to have strong controls in one area if the controls in another are either weak and unreliable or can easily be circumvented. The end result could be the same---a disaster. In view of this and the known interrelationship between various categories of controls, it is necessary that all controls be evaluated prior to rendering an opinion as to the adequacy of computer security within any automated data processing system. Therefore each part of these Proceedings should be considered with equal weight when developing a program for such audits.

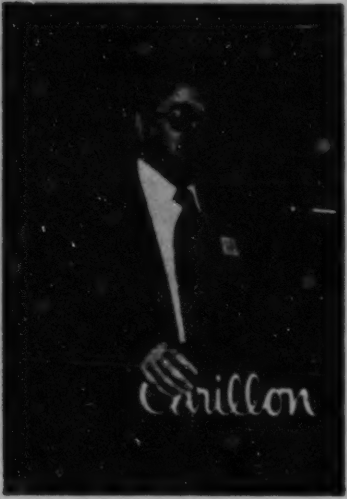
## 2.3 Reading the Proceedings

The reports of the ten sessions are independent of one another and may be read in any order. Note that the reports toward the beginning of the Proceedings are more management oriented while those toward the end are more technically oriented. A detailed Table of Contents has been included as an aid to locating specific materials. Major recommendations and conclusions of the sessions can be found in the Executive Summary at the beginning of these Proceedings. The account of why the Workshop was held, how it evolved, and how the session reports were generated can be found in Appendix B.

# PART II: KEYNOTE ADDRESS

DONALD L. ADAMS
American Institute of Certified Public Accountants

## Biographical Sketch



Donald L. Adams is Managing Director of Administrative Services at the American Institute of Certified Public Accountants, with responsibility for internal applications of the computer as well as development of its use in the accounting and auditing practices of members. His administrative responsibilities include Personnel, Purchasing, Office Management, Printing and Shipping. Long a member of AICPA, he has served on a number of its committees in the computer area, including the chairmanship of the EDP Auditing Committee. He is a former member of the Computer Committee of the New York State Society of CPA's.

Before coming to AICPA in June 1973, Mr. Adams had for three years been Assistant Director of Data Processing at the investment banking firm, Salomon Brothers. Prior to that, he had been Manager of Computer Auditing at Peat, Marwick, Mitchell & Co. He has been involved in computer auditing since 1960, has written many articles on the subject, and has lectured extensively in the United States, Canada and Europe. He is Editor of the monthly newsletter, EDPACS (EDP Audit Control & Security). He studied at Massachusetts Institute of Technology and Syracuse University, earning the B.S. degree Magna Cum Laude from the latter institution in 1959.

Keynote Address
Proceedings of the Workshop on Audit
and Evaluation of Computer Security

Donald L. Adams

## 1. INTRODUCTION

These workshop sessions are quite valuable. They are brief and limited to a stated period of time. This is a positive factor in insuring that they accomplish their goals. Since the time is limited, there is a constraint on the amount of debating that can take place. This is bound to be a help. In many other meetings, we seem to be able to debate topics virtually forever. Having a limited time period means you have a better chance of getting something done. It also means that you do not have time to conduct a survey. Thank God!

It seems that any time a committee addresses a particular problem, the first thing they want to do is conduct a survey. They always seem to be searching for that one elusive nugget of truth that might be buried out there somewhere in the world. Hopefully, a survey might uncover that gem of wisdom. However, I have never known a case where this happened.

Most of us went to school when the scientific method was very much in vogue. As a result, using the scientific approach to problem solving makes us feel comfortable. Unfortunately, accounting and auditing are not sciences. They are at best imperfect art forms. In consequence the application of the scientific method is a mistake. A group, such as the one that is attending this workshop, is hand picked to be a cross section of the most knowledgeable people working in the particular field. It is a good bet that there is not a single important thing going on in the fields of auditing and evaluating computer security that is not known by at least one person attending this workshop. That is where the true value of these workshops comes into play. Knowledgeable people get together, pool their information, and produce a document that will inform others. Used properly, this is a very cost effective way of distributing knowledge. It should be used more often.

## 2. AN APPROACH TO THE WORKSHOP

The outline of the topics to be covered in this workshop includes ten basic areas. It is a very ambitious program. About a year ago, I was involved in a similar effort in regard to the Data Base Directions Workshop. It might be useful to review the approach we used in trying to meet our workshop objectives. The first hour was spent in brainstorming the major topics to be covered. At the end of the hour we listed the projects and voted to select the five that were most important. A time budget was established for each of them. If we allotted five hours to a topic, we discussed it for five hours and then moved on to the next one. The approach worked quite well and it may prove helpful to some of you over the next few days.

## 3. COMMENTS ON PROPOSED TOPICS

I would like to offer a few comments about each of the session topics.

### 3.1 Internal Audit Standards

It is difficult for certified public accountants to establish audit standards. It is even harder for internal auditors to attempt that task. External auditors share a common goal. They are looking to express an opinion on the financial statements of an organization. Internal auditors have a much more variable charter. Their role and the scope of their activities are both established by management. It is difficult for an outside group to dictate standards for the internal audit function. In this particular workshop the approach to be taken in establishing standards depends on how you define security. From the material that was distributed in advance, it appears a very broad definition will be utilized. To the extent that this group is able to develop useful standards, it will be a very positive forward step.

### 3.2 Qualifications and Training

This is another challenging topic. It is very difficult to define the qualifications and training required in the field of computer security since there is no accepted common body of knowledge. Perhaps, a precise definition would be premature. Professional qualifications and standards evolve very slowly. They are coming, but it certainly will be a while before a consensus is formed. It is very hard to predict when we will be able to have meaningful standards for professional qualification in a specialty such as computer security. The group working on this topic should try to keep their recommendations at the general level. It would be a mistake to try and establish a strict set of qualification and training standards this early in the game. It would be better to start slow and build upon that foundation.

## 3.3 Security Administration

This is a relatively new area as it relates to EDP. A thorough discussion of this topic should prove to be quite useful. There is a need for a definition of the duties, responsibilities, and organization of the security administration function. While this material may only be of interest to very large organizations, it will certainly be helpful. We need to develop audit approaches and techniques that can be applied to a review of the security administration function, so guidelines in this area will be particularly useful.

## 3.4 Audit Considerations In Various System Environments

The environment has a decided impact on audit considerations, but what is that impact? This is not an easy question to answer. This group will find they have been given a very tough assignment. Within the current state of the art we cannot be too definitive in providing guidance. To date, no one has done much, if anything, in this particular area. Some thoughtful consideration of this topic should prove to be extremely helpful and will serve as a useful starting point for further work.

## 3.5 Administrative and Physical Controls

This seems to be a strange combination of topics. External auditors would not lump these two together, but it may be useful to consider them in tandem. Yet, it may prove to be a time consuming task. Administrative and physical controls cover a very wide range of topics. The group has been directed to place their emphasis on those areas that are not well defined in the existing literature. They may find it difficult to identify controls that are new or unique.

## 3.6 Program Integrity

Audit approaches and techniques to evaluate the security of operating systems, data base management systems, and application programs are to be covered. The members of this session will consider the problems involved in establishing integrity in these three areas. It is easy to consider the problems, but defining the audit techniques to evaluate integrity will be quite a challenge. The results of this group's deliberations will certainly be of interest.

## 3.7 Data Integrity

This is a more familiar topic. Auditors, particularly external auditors, have been deeply involved in reviewing and evaluating data integrity for quite some time. The group has been asked to identify and discuss data integrity techniques that are not well covered in current literature. This may prove to be a tough assignment.

The literature is quite complete and it will be surprising if the group can develop very much that is new in this area.

### 3.8 Communications

Most auditors lack an in-depth expertise in the field of communications security. The developments of electronic funds transfer systems and distributed processing systems will make this topic one that is of considerable importance. Even if effective security is implemented in all other aspects of a system, the entire ball game could be lost through a data communications security fault. Guidance in this area should prove to be of immense help to the audit community in defining some of its future tasks.

### 3.9 Post Processing Audit Tools and Techniques

A great deal of information is recorded on the journals and logs maintained by most of today's computer systems. Auditors face a major problem in determining what information is available and deciding how to get at it and use it to accomplish and audit. The group has been asked to address the topic of the need for new techniques in this area. They may conclude there is little need for new techniques. Most of the tools that an auditor requires are available. They were developed for use by systems personnel. The auditor needs to develop a familiarity with what is available and to gain experience in its use. The group addressing this topic would accomplish a great deal if they are able to highlight the areas auditors should explore and at the same time, provide guidance as to the tools they might employ.

### 3.10 Interactive Audit Tools and Techniques

In this particular area, the needs of the internal auditor are quite different from those of the external auditor. Internal auditors usually work with more of a managerial emphasis and they are more likely to have a need for on-line analysis of data. CPAs on the other hand, usually perform their work as of a particular point in time. Their needs are usually more static in nature. However, that may change. The growth of EFTS and distributed processing may make interactive auditing a more important area. Both internal and external auditors will be interested in the deliberations of this group.

## SUMMARY

The session theme, Audit and Evaluation of Computer Security, is a timely one. The topics that have been proposed for discussion are all of current interest and deal with areas that are of importance to the audit community. To date, the known financial losses related to data security failures are quite small. However, logically, these losses are bound to increase. Consideration of the topics outlined for this workshop will provide a better basis for defining our current problems and developing the techniques we will need to cope with an expanding technology.

## PART III: INTERNAL AUDIT STANDARDS

Chairperson: William E. Perry
The Institute of Internal Auditors

Participants:

Howard R. Davia
General Services Administration
S. Jeffery
National Bureau of Standards
Fred L. Lilly
Lilly & Harris, CPAs
Gerald E. Meyers
CNA Insurance

Kenneth A. Pollock
U.S. General Accounting Office
Frank S. Sato
Department of Defense
Donald L. Scantlebury
U.S. General Accounting Office
T. Q. Stevenson, Recorder
Department of Agriculture

From left to right: T. Q. Stevenson, Donald L. Scantlebury, Kenneth A. Pollock, Howard R. Davia, William E. Perry, Gerald E. Meyers, Fred L. Lilly, S. Jeffery, Frank S. Sato

---

Note: Titles and addresses of attendees can be found in Appendix A.

## EDITORS' NOTE

A breif biography of the Session Chairperson follows:

Mr. William E. Perry is the Director of EDP and Research for the Institute of Internal Auditors and serves as staff liaison for the International Committees on EDP Auditing and Research. Prior to joining the Institute, he was Supervisor of Corporate Computer Auditing for Eastman Kodak Company. He has also held positions with Arthur Young & Company, Ft. Richie, and Price Waterhouse & Company. He is a graduate of Clarkson College, holds a MBA from Rochester Institute of Technology and a MEd from the University of Rochester. He is a Certified Public Accountant (NY) and a Certified Internal Auditor. He is a member of the Computer Services Executive Committee and the Auditing Advanced EDP Systems Task Force of the AICPA, a member of the Board of Directors of the American Federation of Information Processing Societies, and past committee chairman of the GUIDE International PL/1 Committee. He was a professor of data processing at Monroe Community College. His most recent publications include: "Pre-Occurrence Auditing--Building Control Into the Audit Program," Bank Administration (Jan. & Feb., '75) and numerous contributions to EDPACS on subjects of EDP audit and control.

---

The charge given to this session was:

> INTERNAL AUDIT STANDARDS: Develop a proposed statement of audit standards for computer security considering (a) the role of the internal auditor, and (b) application of traditional audit standards.

Computer security is a very complex subject that must be considered from a total system perspective. It involves all the controls necessary to ensure (1) the accuracy and reliability of the data maintained on or generated by an automated data processing system, and (2) the protection of the organizational assets to include the hardware, software, and data from all anticipated threats or hazards.

This session is to consider the responsibilities of the internal auditor in evaluating computer security throughout the developmental and operational life cycle of an automatic data processing system. The AICPA's Statement on Auditing Standards No. 3 entitled, "The Effects of EDP on the Auditor's Study and Evaluation of Internal Control" should be considered for use as a departure point for this session.

---

The consensus report that follows was developed and reviewed by the majority of the membership of this session.

# Supplemental Standards for Internal Auditor's Expanded Role in Reviewing Computer Systems and their Development
## A Consensus Report

William E. Perry, Fred L. Lilly, D. L. Scantlebury,
Ken Pollock, T. Q. Stevenson, Frank S. Sato

## 1. INTRODUCTION

### 1.1 Automated Systems Effect on Environment

The computer has substantially altered the methods by which data processing systems operate and are controlled and audited. The opportunities for personal review and clerical checking have declined as the collection and subsequent uses of data are changed. The changes are the result of moving from manual procedures performed by individuals familiar with both the data and the accounting process to high volume, automated techniques performed by individuals unfamiliar with both the data and accounting practices.

The introduction of data processing equipment frequently requires that the recording and processing functions be concentrated in departments that are separate from the origin of the data; it may, however, eliminate the separation of some of the responsibilities that previously characterized the record keeping function. A trend toward the integration of operating and financial data into organization-wide information systems of data bases also eliminated independent records that might previously have provided a source of comparative data. At the same time, such integrated information systems can become the basis for more vital and timely management decisions.

Computerization has reduced substantially the time available for the review of transactions before their entry into the accounting records. As a result, in poorly controlled systems the opportunity for discovering errors or fraud before they have an impact on operations may be reduced, especially in the case of real-time and data base systems. This has increased the importance of internal control procedures [1]. It also affects the work the auditor must perform. An important aspect of this work is reviewing the adequacy of computer security.

### 1.2 Computer Security Defined

Computer security is a very complex subject that must be considered from a total system perspective. It involves all the controls necessary to ensure (1) the accuracy and reliability of the data maintained on or generated by an automated data processing system, (2) an appropriate degree of protection of the organizational assets to include the hardware, software, and data from all significant anticipated threats or hazards, and (3) the economy and efficiency of computer operations.

Computer security does not include (1) the justification of a computer system, (2) the full range of meeting all management objectives, and (3) determining an acceptable level of risk for an organization, but all are areas for audit involvement.

## 1.3 Discussion of Audit Involvement in Computer Security

The concept of accountability is inherent in government and non-government audits. Any audit could encompass the three elements bearing on accountability, which are:

1. Finance and compliance

2. Economy and efficiency

3. Program results

From the standpoint of the auditor reviewing security, the elements of both compliance and program results are within bounds. (Efficiency and economy may be adversely affected by a tight computer-security requirement.) There may be specific standards or regulatory requirements governing security aspects of an operation which should be reviewed for compliance, and in evaluating the program results of an operation, security may be an important factor. Similarly, in audits performed by CPA firms and the GAO, attention is given to the adequacy of control over assets, and this may well involve the security controls over information held by the organization. Internal auditors should be concerned with the adequacy of control of organization-held information.

A separate auditing standard per se to cover the auditor's work in this area is not warranted. However, another mechanism is needed to draw the auditor's specific attention to the problem of computer security and make him aware of his responsibilities. The mechanism may include items such as a commentary, clarification, or interpretation of existing standards.

The AICPA used this means when it issued Statement of Auditing Standards (SAS) No. 3 "The Effect of EDP on the Auditors' Study and Evaluation of Internal Control." The basic CPA audit standards which have served so well without modification for so long were not changed with the advent of the computer, but the SAS amplified and interpreted the standards as it related to EDP. We have chosen to use the term "supplemental standard" in discussing the expanded role of the internal auditor in this area.

### 1.4 Changing Auditor Requirement

When internal auditors function in a computerized environment, their audit responsibility needs to encompass the following:

1. Provide guidance to data processing and user personnel for creating the mechanism for auditable systems
2. Determine that internal controls in computerized applications are operative and effective by reviewing and testing those controls.

## 2.0 SUPPLEMENTAL STANDARDS FOR COMPUTER INTERNAL AUDIT WORK

### 2.1 General

A computerized environment does not create a need for new audit standards. The current internal audit standards as set forth in the GAO pamphlet "Standards for Audit of Governmental Organizations, Programs, Activities, & Functions," are basically appropriate for audits of the data processing function. What is needed are supplements to those standards that specify the additional tasks the auditor must perform in a computerized environment to meet the basic standards.

Three areas have been identified for the purposes of supplementing those standards. These are audit involvement in:

1. Systems development
2. Operational systems (application controls)
3. Physical security and general controls

### 2.2 Supplemental Standard for Systems Development

The internal auditor shall be involved in the development of new data processing systems or significant modification of existing ones with the objectives of seeing that such systems:

1. Include the controls necessary to protect against theft and serious error
2. Provide the audit trails needed for management, auditors, and operational review
3. Faithfully carry out the policies management has prescribed for the system

4. Will provide an efficient and economical system

5. Are in conformity with applicable legal requirements

6. Are documented in a manner that will provide an understanding of the system required for maintaining and auditing the system

### 2.2.1 Commentary

The system development process includes the definition of processing applications to be carried out by a computer, design of the processing steps to be followed, determination of the data input and files that will be required, and specifications for individual program's input data and output.

Auditor involvement is important in the design of an application. It is needed because the design must provide for necessary control procedures and produce the reports and data files which will be needed for audit purposes after the system becomes operational.

Requirements for an EDP system should be established by management and it is the auditor's responsibility to determine whether or not these policies are being carried out in the design and whether or not the design conforms with applicable legal requirements. This will require the auditor to ascertain the nature of the requirements set by management, and whether or not the requirements are being met.

The auditor should ascertain that an appropriate approval process is being followed in development of new systems and making modifications to existing systems. In doing this the auditor should consider the need for approval of system design by data processing management, user groups, and other user groups whose data and reports may be affected.

The auditor should also determine whether or not management requires documentation sufficient to define the processing that must be performed by programs in the system, data files to be processed, reports to be prepared for users, operating instructions for use by computer operators, and user group instructions for preparation and control of data, The auditor should also ascertain whether or not management policy provides for testing sufficient to give assurance that reliance can be placed in the system before the system is used for production purposes.

The auditor should review provisions for security required by management to protect data against unauthorized access and modification. The auditor should also consider whether the benefits of the system justify its costs whenever the benefits can be quantitatively measured. In all cases, the auditor should be alert to whether the system design will provide for an economical and efficient system and should investigate instances in which it appears more economical or efficient methods can be used.

After reviewing management policies, the auditor should examine approvals, documentation, test results, and cost studies and other data to determine the extent to which management policies are being followed. The auditor should keep a close association with the system during the development phase [2] but should not become a part of the design team--except to the extent of recommending controls--in order to maintain proper objectivity.

The auditor should report in writing on both the adequacy of the policies and the extent to which those policies are being followed as determined by the auditor's examination. The auditor should specifically comment on all findings which require corrective action and should, to the extent possible, submit recommendations for appropriate action.

### 2.3 Supplemental Standard for Operational Systems (Application Controls)

The internal auditor should review the installed data processing applications to determine reliability in processing data in a timely, accurate, and complete manner.

Audit objectives should be to:

1. Determine whether the installed application conforms to standards and the latest approved design specifications, and
2. Disclose possible weaknesses in the installed application through periodic audits designed to test internal control and the reliability of the data produced.

### 2.3.1 Commentary

The transition from mechanical data processing (MDP) to electronic data processing (EDP or ADP) occasions the need for revision in traditional audit standards. More specifically, the complexity and far-reaching scope of EDP systems require that the internal audit give greater attention to the system which processes data, as well as to the data; the theory being that, if the system is secure, the data processed and reported will be reliable.

Supplemental standard one deals with the internal auditor's involvement in the development of the system specifications for the purpose of assuring that computer security has been adequately considered--with an appropriate risk analysis--and that the more traditional internal controls over data processing are included.

Audit compliance with supplemental standard two provides assurance that the approved specifications, with all built-in internal controls, etc., have been installed as intended on specific applications.

It further provides that the auditor institute periodic internal audits designed to probe the installed application for weaknesses, changed circumstances in risk exposure, etc., with the intention of stimulating corrective modifications of specifications and improving the installed applications. In these periodic audits, the internal auditor's consideration of internal controls is particularly important. Also, the auditor must be mindful, when conducting periodic tests of the installed system, that there are no guarantees that the system will continue to operate in accordance with the latest approved specifications.

As a part of the testing of reliability of data produced, the auditor will normally examine supporting documentation for selected transactions and test the clerical accuracy of the manner in which transactions have been entered and summarized and to test compliance with control procedures. In addition, auditors may wish to test selected data files to identify possible exception conditions and accuracy of data conversion or capture. If the data records are maintained in machine-readable condition, the auditor should, where appropriate, make use of computer assisted audit techniques in testing data records.

Because of the significant potential for fraud and other irregularities in computer systems, the internal auditor must be alert to the potential of fraud. Although auditing for fraud should not necessarily be the primary objective, the current environment dictates that detection of major frauds should be one of the objectives of internal auditing.

## 2.4 Supplemental Standard for Physical Security and General Controls

The internal auditor should be involved in review of the general controls present in data processing systems to assure that their existence and operation are in accordance with management direction and legal requirements, and are operating effectively to provide security over the data being processed.

### 2.4.1 Commentary

The auditor should distinguish between general EDP controls, which are normally applicable to all processing being carried out within the installation, and application controls (covered in Section 2.3), which may vary between applications and are therefore reviewed on an individual application basis. In reviewing general controls, auditors review and evaluate controls in several areas, and consider the effectiveness of the general controls in performing the review of application controls.

Authority and responsibility must be delegated within the organization in such a manner that the objectives of the organization can be met with efficiency and effectiveness. The auditor should review the organization, delegation of authority, responsibilities, and separation of duties in the organization to determine whether or not functional lines of authority are designed to meet the organization's objectives, and whether or not the separation of duties provides for a relatively strong level of internal control. Separation of duties should provide for separation between program and systems development functions, computer operations, control over input of data, and control group responsible for maintaining application controls.

In reviewing the separation of duties, the auditor should evaluate the control strengths, and report on any weaknesses resulting from inadequate separation of duties. The separation of duties may be enhanced by policies requiring periodic rotation of duties and mandatory vacations. The auditor should also review whether such policies are being followed.

Adequate physical facilities and other resources (such as adequately trained personnel, supplies, and power) are necessary for the organization to meet its processing objectives. The auditor should review these facilities to determine whether or not the organization has adequate facilities for meeting its needs.

Personnel management, including supervision of personnel, motivation of personnel, and professional development is an integral part of the successful management of the data processing function. The auditor should review these policies to ascertain whether or not the necessary management policies exist and determine whether or not they are properly followed.

The auditor should review provisions for physical security of the computer hardware, computer programs, data files, and personnel to ascertain the extent of security being maintained. This review should include not only the computer equipment present in the central processing facility, but also extends to computer terminals and other peripheral equipment. In reviewing physical security of computer hardware, the auditor should consider the extent to which there are adequate contingency plans for continuity of processing in the event of a disruption of data processing functions. This should include not only provisions for hardware backup but detailed plans for making use of backup equipment, transporting personnel, programs, forms, and data files to an alternate processing location, and other contingency plans necessary for this mode of operation. The auditor should also consider the extent to which this contingency plan has been exercised.

In reviewing physical security over files, the auditor should determine whether or not data and program file libraries are maintained by personnel who do not have access to computers and computer programs, whether or not the library is secure, whether or not computer operators and other personnel have access to the library, and provisions for backup of files (including off-site backup). In the case of files normally maintained on-line, the auditor should consider the extent to which these files are protected by authorization controls within the operating system and whether backup copies of files are maintained on a regular basis. As a part of the review of procedures for maintaining backup copies of files, the auditor should review procedures for ensuring that backup files are properly identified, labeled, and contents verified to ensure that the backup medium is complete and accurate.

Since computer systems are most often controlled by systems software and particularly operating systems, and since systems software provides for file handling capabilities, multiprogramming capabilities, file label checking, and many other authorization controls, the systems software is an integral part of the control over computer processing. The auditor should be aware of the types of controls which the operating system and other systems software can exercise and should ascertain the extent to which those controls have been implemented. As a part of this review, the auditor should be aware of the fact that personnel responsible for maintenance of the systems software, and other persons with the ability to make unauthorized modifications to this software, may either intentionally or accidentally cause specific control features within that software to become ineffective.

Computer hardware frequently has capabilities designed into it for detection of erroneous conditions related to hardware malfunctions rather than program malfunctions. The auditor should be aware of the extent to which the installation relies upon these hardware controls, the extent to which the operating system utilizes these controls, and the manner in which hardware errors detected in a system are reported within the installation as well as procedures for taking corrective action.

### 2.5 Other Audit Requirements

The auditor should review the organization's economic justification and analysis for procurement of all data processing equipment. This will include a thorough review of the cost-benefit analyses developed by the data processing staff in conjunction with users of systems that are to be operated. The cost justification developed by management should encompass a reasonable level of risk analysis to assure that the equipment being purchased is in fact commensurate with the needs and probability of exposure or loss. For example, it may be that the requirements to comply with the Privacy Act may necessitate adoption of special techniques to prevent accidental or intentional disclosure of data. This may be accomplished in a number of ways; the method chosen should be that which is most cost effective for the intended purpose.

## 3.0 RECOMMENDED COURSE OF ACTION

The auditor should review the organization's ADP system acquisition document for its standards. These specifications then should be compared to any applicable ones of the organization and to what is actually implemented on the operating equipment and software. Any deviations should be documented by an approved waiver or other release.

The following three actions are suggested for fostering the acceptance and implementation of the previously stated three supplemental internal auditing standards.

1. That GAO review these standards and consider modifying their standards pamphlet accordingly, or issuing separate supplemental material encompassing the supplemental standards.
2. That the supplemental standards be presented to the Federal Audit Executives Council for review and endorsement.
3. That NBS consider these supplemental standards in preparing FIPS guidelines for systems development, operational systems, physical security and general controls.

## 4.0 REFERENCES

[1] Elise G. Jancura and Fred L. Lilly, "SAS No. 3 and the Evaluation of Internal Control." The Journal of Accountancy, March 1977, page 69.

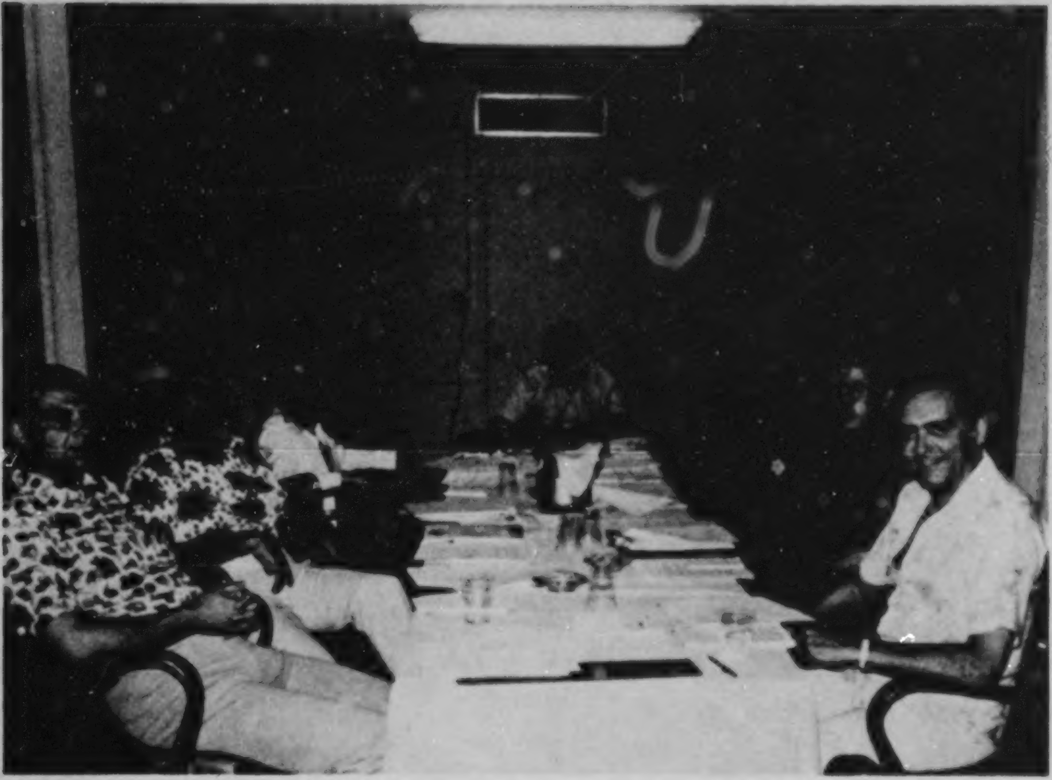
[2] Federal Information Processing Standards Publication 38, Documentation of Computer Programs and Automated Data Systems. Superintendent of Documents, Government Printing Office, SD Catalog Number C13.52:38.

## PART IV: QUALIFICATIONS AND TRAINING

Chairperson: C.O. Smith
U.S. General Accounting Office

Participants:

| | |
|---|---|
| Sid Baurmash<br>Seidman & Seidman | Walter Kennevan<br>American University |
| Adolph Cecula<br>U.S. Geological Survey | Kathleen Kolos, Recorder<br>Central Intelligence Agency |
| C.W. Getz<br>General Services Administration | Herman McDaniel<br>U.S. Civil Service Commission |



From left to right: Adolph Cecula, Sid Baurmash, Kathleen Kolos, C.O. Smith, Walter Kennevan, Herman McDaniel, C.W. Getz.

---

Note: Titles and addresses of attendees can be found in Appendix A

# EDITORS' NOTE

A brief biography of the Session Chairperson follows:

Mr. C. O. Smith is an Assistant Director of the Logistics and Communications Division of the United Stated General Accounting Office in Washington, D.C. He has over 20 years of broad and in-depth experience working with all levels of operating and management personnel within Federal, state, and local governments, and private industry. He is responsible for planning, directing, coordinating, and participating in world-wide evaluations of information handling operations involving administrative, scientific, and military applications of computers. His work has concentrated on assessing all aspects of information handling including system and program project planning, management analysis, design, implementation, and operation on a world-wide basis. During the past 10 years he has focused on a wide variety of different systems and programs including but not limited to command and control, payroll, accounting, logistical, and management information applications. Previously he specialized in assessing the performance of individual data processing installations. His degrees are in Accounting (California State University-Fresno, B.S.) and in Business Administration and Management Information Systems (The American University, M.B.A.). He is a Certified Internal Auditor (CIA) and member of the Institute of Internal Auditors, the Society for Management Information Systems, Military Operations Research Society, and the EDP Auditors Association, Inc. His most recent pertinent publication, with H. J. Podell and B. Knowles, is Management Auditing of Computer Operations: A Tutorial, New York, IEEE, Inc., 1976.

---

The charge given to this session was:

QUALIFICATIONS AND TRAINING: What are the qualifications and training necessary to conduct audits of computer security?

The first general auditing standard of the AICPA is as follows: "The examination is to be performed by a person or persons having adequate technical training and proficiency as an auditor." (SAS No. 1, section 150.20). SAS No. 3, paragraph 4, expands on this standard by stating that, "Situations involving the more complex EDP applications ordinarily will require that the auditor apply specialized expertise in EDP in performance of the necessary audit procedures."

The task of this session is to identify and define the specialized expertise necessary to conduct evaluations of computer security together with the training and experience needed to achieve the appropriate level of expertise. Consideration should be given to the full spectrum of controls from the evaluation of simple physical safeguards to an analysis of the protective features of system software.

---

The consensus report that follows was developed and reviewed by the entire membership of this session.

## INTRODUCTION

The computer is rapidly becoming one of our most useful tools. In the slightly more than two decades since its introduction, the computer has made a profound change in many facets of our lives. It assists us in predicting the outcome of our elections; it guides our astronauts in space to compensate for man's relatively slow reaction time; it controls the flow of our traffic on the streets, on rails, and in the air; it is used to help diagnose our ills; forecast our weather; compute our bank balances; and hundreds of other chores which we could not even undertake before its advent.

Predictions on the future use of the computer are many and varied because the ingenuity of man knows no dimensions of time when dealing with the possibilities of pressing back the frontiers of his ignorance. Since the expected growth in the use of the computer will contine to be nothing less than phenomenal, managers and other users will tend to become much more dependent on the computer than they have been in the past. As these individuals become more dependent on the computer, opportunities for its misuse and abuse will also increase. As the opportunities for computer misuse and abuse increases, managers and those individuals who will audit and evaluate computer operations, particularly computer security, must be highly qualified and well trained. These individuals must be familiar with the symptoms of potential disaster so that efficient and effective corrective action plans may be initiated, implemented, and maintained before their computer systems become a nightmare of error and financial loss. In addition, these individuals must be familiar with the methods used to protect data from all anticipated threats or hazards.

For these reasons, the basic question addressed during this session of the workshop was "What are the qualifications and training an individual needs to conduct reliable audits of computer security?" Specifically, this task consisted of identifying and defining the specialized expertise necessary to properly conduct evaluations of computer security together with the requisite training needed to achieve that level of expertise. Stated more simply, What is the common body of knowledge needed to do this work?

## CONSIDERATIONS ASSOCIATED WITH DEVELOPING A COMMON BODY OF KNOWLEDGE

For our purposes, the panel considered computer security from a total system perspective; that is, computer security involves all the controls necessary to ensure the integrity, accuracy, and reliability of the data that is an integral part of an automated data processing system. This perspective includes all the controls established over the acquisition, processing, storing, and dissemination of information. The panel tempered their consideration with the knowledge that they were unaware of any foolproof system of evaluating computer security that will prevent an unauthorized or illegal intervention or penetration of an automated data processing system by a sophisticated professional and technically qualified intruder.

When considering the appropriate level of expertise necessary to conduct these audits, the panel first attempted to identify the common body of knowledge that an individual must have before becoming involved in this work and then gave extensive consideration to the complexities of the environment in which the individual would conduct the work. The panel assumed that the individual(s) conducting these evaluations could have their basic education and experience in any generally recognized discipline such as, but not limited to, accounting, business administration, engineering, operations research, computer science, or economics. Each of these disciplines already has a specified body of knowledge identified or associated with it. Since individuals with varying backgrounds and experience can be expected to conduct these evaluations, the panel could not assume that everyone undertaking this work would be a fully-qualified professional auditor. Regardless of an individuals' basic education and experience, audits of computer security demand a solid foundation in the concepts and practices of management and auditing supplemented by a solid foundation in the fundamentals of data processing and telecommunications, including an appreciation of hardware and software capabilities and limitations. Depending on the type, nature and scope of the audit, an individual will require varying degrees of knowledge and experience in computer operations, software performance, and information flows into, through, and out of the automated data processing function. The more complex the system being evaluated the more comprehensive technical knowledge will be required. For example, if a major segment of the audit is to ascertain the integrity of a computer program or a series of computer programs the auditor, among other things, should be thoroughly familiar with the severity of the potential or real threats that can be mounted against them. As outlined in Part VIII of the Proceedings, these threats include but may not be limited to the following:

A. Accidental disclosure
   1. Natural failure of either or both hardware and software
   2. Human error

B. Casual unauthorized access
   1. Browser discovered flaws
   2. Exploiter (intruder) seeks flaws

C. Deliberate attack
   1. Thief creates flaws (plants trap doors, modifies code)
   2. Conspiracy (the conduct of a planned attack)
   3. Irrational employee

Frequently the skills needed to conduct this type of audit do not reside with a single individual. In this situation multidisciplinary audit teams could be used. A multidisciplinary team contains all the skills and experience needed for a specific audit. The multidisciplinary team approach has been used very successfully by both governmental and non-governmental organizations.

In addition, it was the panel's view that they should not overly concern themselves with "who will conduct the audit" and that they should concentrate their efforts on identifying the common body of knowledge needed to do the work. Further, the panel did not concern themselves with "who would provide the training." It was the panel's view that universities; colleges; the Civil Service Commission; the Interagency Auditor Training Center; the Institute for Professional Education, Inc.; and a myriad of other institutions and professional organizations either have or could develop courses, seminars, or workshops that would meet the training and educational needs included in that common body of knowledge.

Finally, the panel did not attempt to ascertain the costs involved in developing the needed level of expertise because too many variables are involved. For example, the costs associated with developing the needed level of expertise will vary substantially depending on whether the organization: develops the capability in-house by training their own employees, partially develops the capability in-house by training a few selected employees and supplementing this capability by temporarily hiring the additional expertise from a source outside the organization, or hires, either temporarily or on a continuing basis, the needed expertise from an outside source such as a consulting firm. Since each organization and each individual will have different training needs, an organization must develop its own program to obtain and maintain the common body of knowledge needed to effectively audit computer security. Perhaps a major concern here is not how much does it cost to develop the needed level of expertise, but whether the organization can afford not to develop it in the light of the increasing number of detected and reported cases of computer misuse and abuse.

When developing the common body of knowledge needed for auditing computer security, the panel was confronted with two basic problems. First, there is the problem of enhancing the basic knowledge and experience of those who will conduct the audits; and second, there is the problem of determining the extent of the technical training needed by each individual participating in the audit. Experience has shown that there are at least three levels of knowledge required for this work. There is a general level of knowledge required in the disciplines of management and auditing concepts and practices. Individuals graduating from a recognized university or college with a degree in business administration or accounting will usually have reached this level of knowledge. These individuals will generally lack a solid foundation in the fundamentals of data processing and telecommunications and will have to acquire this knowledge through additional training.

The second level of knowledge requires an individual to develop a solid foundation in the fundamentals of data processing and telecommunications including an appreciation of hardware and software capabilities and limitation. An individual graduating from a recognized university or college with a degree in a discipline such as computer science will normally have attained this level of knowledge. Such an individual may lack a solid foundation in management and auditing concepts and practices and will have to acquire this knowledge through additional training.

The third level of knowledge involves the development of a comprehensive technical knowledge and the related experience to audit the more sophisticated aspects of a computer system. For example, this level of knowledge would be required when evaluating the vulnerability of an operating system (monitor, executive system, etc.) for unauthorized access by a browser or skilled exploiter seeking flaws in the system.

With these requirements in mind, the panel outlined the common body of knowledge and the related qualifications and training they believed to be necessary to conduct reliable audits of computer security. The outline beginning on page 4-11 has been preceeded by a brief description of the importance of each part of that body of knowledge.

For purposes of guiding the reader the outline has been divided into eight parts as follows:

1. Computer systems, operations, and software
2. Data Processing techniques
3. Management of the data processing function
4. Security of the data processing function
5. Risk analysis and threat assessment
6. Management concepts and practices
7. Auditing concepts and practices
8. Additional qualifications needed to audit computer security

## 1. COMPUTER SYSTEMS, OPERATIONS, AND SOFTWARE

The topics covered in this section are intended to provide a broad theoretical foundation necessary for an individual to understand the interrelationships and interactions of all parts of a computer system. The foundation provided by these topics will give an individual a familiarity with the way computers operate and the interrelated and essential function of software. These general principles may be applied to any type of system regardless of whether it is a batch, interactive, on-line or distributive system.

## 2. DATA PROCESSING TECHNIQUES

Dramatic advances in data processing techniques have taken place within the past two decades and each year brings still faster and more efficient methods for processing data. Programming languages have proliferated, data management has become more efficient and file processing techniques have made it possible to store and retrieve vast amounts of data. This rapid evolution of data processing requires an individual not only to have a basic understanding of data processing techniques, but to maintain currency in this rapidly changing field.

The topics in this section cover, in a general way, the essentials of data processing techniques. They cover the techniques currently in use in the field and must be maintained with an on-going program of education because of the speed with which new developments are taking place.

## 3. MANAGEMENT OF THE DATA PROCESSING FUNCTION

Good management of the data processing function is one of the key elements in providing reliable security of computer operations. In addition to being responsible for day-to-day operations, these managers must also concern themselves with a myriad of other details ranging from the physical layout of their operations to the reliability of the software used to process data. The importance of these tasks cannot be overemphasized. The interrelationship of these tasks and their contribution to the management of on-going programs must be understood by the auditor.

The topics in this section introduce the "auditor" to the basic areas of responsibility associated with managing the data processing function. These topics also assist the "auditor" in placing the data processing function into appropriate perspective within the organization as a whole. In this respect the computer is the processor of information not the creator or user of information at least in a managerial sense. Finally, these topics will help the auditor understand the contribution this function makes in the management of on-going programs.

## 4. SECURITY OF THE DATA PROCESSING FUNCTION

Although there are no security techniques so foolproof that they will prevent a determined and technically skilled intruder from penetrating a computer system there are certain measures that can be taken to discourage penetration. These safeguards will vary from installation to installation depending on a number of factors such as the sensitivity or classification of the data, the clearance level of personnel, and perimeter control to name a few. An individual must be familiar with security techniques as well as the sensitivity of the data in a computer system to be able to make reliable evaluations of how adequately the data is being protected. The development of a remote access capability for computer systems has added to the difficulty of maintaining effective security. Part of an individuals' task will be to assess the adequacy of security for all components of a computer system.

The topics contained in the outline are intended as a starting point, a listing of those security measures that should be used. This listing is not intended to be exhaustive of those measures only illustrative of them and should be used as a base on which to devise new and more effective methods and to build a greater knowledge of this subject.

## 5. RISK ANALYSIS AND THREAT ASSESSMENT

Managers and individuals evaluating computer operations must be able to recognize the symptoms of potential disaster. Knowing the probability of the occurrence of a particular threat is a major factor in evaluating the type and nature of the security procedures that will be most effective against it. Threats may come from any direction such as natural hazards (floods or fire) or personnel who may accidentally or deliberately interfere with the proper operation of a computer system. In order to be able to evaluate security techniques and procedures an individual must be able to assess the extent of damage that could result from a disaster. Thus, an individual should have a basic understanding of risk analysis techniques in order to make realistic assessments of potential damage.

The list of topics in this part of the outline are intended to provide the basic understanding of the risk analysis techniques needed to do this work effectively.

## 6. MANAGEMENT CONCEPTS AND PRACTICES

Most authorities view the task of managing slightly differently. Perhaps this difficulty is due to the different environmental situations in which they have worked or perhaps it is due to their own temperamental characteristics which have led them to develop certain methods of managing which, for them, have proven to be effective.

Part of the difficulty also may be due to the fact that the art and science of managing has been undergoing considerable change since mid-century. Mathematical and statistical concepts, the computer, and the developing behavorial sciences, to name a few, have had a tremendous impact on the concepts and methods of managing. There are no simple formulas or pat answers for managing. Managing is much too complex a task for that. However, even though authorities view the task of managing differently they are unanimous in their endorsement of the topics associated with the task. Those topics have been included in the panel's outline of the common body of knowledge needed to audit computer security.

## 7. AUDITING CONCEPTS AND PRACTICES

The techniques of auditing and the related topics form the foundation for conducting evaluations of computer security. Auditing, per se, is almost as old as civilization. It was used in ancient Egypt. the Roman Empire, and, of course, the great mercantile establishments of the Middle Ages. The common areas of audit action throughout its history have been examining, verifying and reporting. Auditing has become a key factor in controlling every kind of organization and its importance has only increased since the advent of the computer. For example, Jack Brooks, Chairman, Committee on Government Operations, House of Representatives recently stated that the lack of utilization reviews was one of the basic problems in the Federal Government[1].

Since the advent of the computer, the potential threats to which information can be subjected, whether by accidental disclosures, casual but unauthorized access or by deliberate attack have increased tremendously. Thus, the need to continually audit computer security cannot be overemphasized.

The topics included in this section of the common body of knowledge are those most commonly associated with the field of accounting. They provide both the auditor and the non-auditor a solid foundation in the principles and practices of auditing an essential ingredient to the team conducting evaluations of computer security.

## 8. BASIC QUALIFICATIONS NEEDED TO EVALUATE COMPUTER SECURITY

The qualifications identified by the panel represent those experience factors an individual should possess in addition to a solid foundation in management, auditing concepts and practices, data processing, and related telecommunications.

It was the general consensus of the panel that an individuals basic education and experience must be supplemented by approximately one additional academic year or equivalent of education in the subjects considered to be the essential components of the common body of knowledge needed for this work. This additional education represents about 400-500 classroom hours of effort. For purposes of comparison, each classroom hour was considered to be 50 minutes in duration. A one semester-three unit college course would meet three times each week for 14-16 weeks. Such a course would represent 42-48 classroom hours of work. Also, it may take an individual one to five years of on-the-job training or practical experience in auditing computer security before they become highly efficient and effective in this work.

---

[1] Administration of Public Law 89-306 Procurement of ADP Resources by the Federal Government, Thirty-Eighth Report by the Committee on Government Operations together with Additional Views, House Report No. 94-1746, October 1, 1976.

## SUMMARY

Since the computer is rapidly becoming one of our most useful tools and the predictions on its future use are many and varied, it becomes increasingly important that managers and other users are able to rely on the products it produces. As these individuals become more dependent on its use they will tend to rely more heavily on the information provided them by individuals conducting audits of their computer security, so that their computer operations will become an ally rather than a nightmare of error and financial loss. For these reasons the individuals conducting these audits must be highly qualified and well trained. The common body of knowledge outlined below is intended to be a basis for developing the needed level of expertise.

# OUTLINE

## COMMON BODY OF KNOWLEDGE NEEDED TO AUDIT COMPUTER SECURITY

1. COMPUTER SYSTEMS, OPERATIONS, AND SOFTWARE
   - A. Theory of systems (as applied to information systems)
   - B. Theory of computers
   - C. Theory of data communications

2. DATA PROCESSING TECHNIQUES
   - A. Information structures
   - B. Programming languages
   - C. Sort and search techniques
   - D. File creation, maintenance, and interrogation
   - E. Storage devices
   - F. Data management systems
   - G. Integrated systems
   - H. The dynamics of developing, modifying, and maintaining computer software

3. MANAGEMENT OF THE DATA PROCESSING FUNCTION
   - A. Organizational structures
   - B. Personnel selection, training, and management
   - C. Operating and organizational policies and procedures
   - D. Computer operations
   - E. Analysis, design, and programming functions

4. SECURITY OF THE DATA PROCESSING FUNCTION
   - A. The computer center
   - B. Remote sites
   - C. Systems including operating, application, and telecommunications software
   - D. Policies and procedures
   - E. Personnel
   - F. Data handling
   - G. Recovery capabilities
   - H. Tests of internal controls

5. RISK ANALYSIS AND THREAT ASSESSMENT
   - A. Physical facilities
   - B. Remote sites
   - C. Software
   - D. Information

6. MANAGEMENT CONCEPTS AND PRACTICES
   - A. Management tasks, responsibilities, practices, and ethics
   - B. Business administration
   - C. Principles of organizational structures
   - D. Concepts of general management
   - E. Management of the human resource

### 7. AUDITING CONCEPTS AND PRACTICES

A. Introductory accounting
B. Intermediate accounting
C. Advanced accounting
D. Cost accounting
E. Municipal and governmental accounting
F. Auditing

### 8. ADDITIONAL QUALIFICATIONS NEEDED TO AUDIT COMPUTER SECURITY

Individuals selected to conduct audits of computer security, in addition to the common body of knowledge outlined above, should have the following qualifications:

1. Sufficient experience to be able to plan, direct, and coordinate audits of large complex functions, activities, or programs,
2. The ability to assign tasks to individuals on the team and to identify the specific disciplines and expertise needed to perform the work, and
3. The ability to conduct conferences and to prepare, present, and process the report describing the results of the work.

# BIBLIOGRAPHY

Allen, Brandt R. "Computer Security." *Data Management* 10 (February 1972): 24-30.

American Institute of Certified Public Accountants Auditing Standards Executive Committee. *Effects of EDP on the Auditor's Study and Evaluation of Internal Control*. New York: American Institute of Certified Public Accountants, 1974.

Campbell, Voin R. "Privacy and Security in Local Government Infosystems." *Infosystems* 23 (December 1976): 31,34.

Canadian Institute of Chartered Accountants. *Computer Audit Guidelines; Guidelines on the Minimum Standards and Accepted Techniques Which Should be Observed in the Audit of Organizations Using a Computer.* Toronto: Canadian Institute of Chartered Accountants, 1975.

Canadian Institute of Chartered Accountants. *Computer Control Guidelines; Guidelines on the Minimum Standards of Internal Control Which Should be Maintained by Organizations Using a Computer*. Toronto: Canadian Institute of Chartered Accountants, 1970.

Canning, Richard. "The Internal Auditor and the Computer." *EDP Analyzer* 13 (March 1975): 1-13.

Cardenas, Alfonso F.; Presser, Leon; and Marin, Miguel, eds. *Computer Science*. New York: John Wiley & Sons, 1972.

Cutting, Richard W.; Guiltinan, Richard J.; Lilly, Fred L.; Mullarkey, John F. "Technical Proficiency for Auditing Computer Processed Accounting Records." *Journal of Accountancy* 132 (October 1971): 74-82.

Gildersleeve, Thomas R. *Data Processing Project Management*. New York: Van Nostrand Reinhold Co., 1974.

Gray, Max, and London, Keith. *Documentation Standards*. Princeton: Brandon/Systems Press, 1969; revised ed.,New York: Petrocelli Books, 1974.

Hamphill, Charles F., Jr., and Hamphill, John M. *Security Procedures for Computer Systems*. Homewood, Ill: Dow-Jones-Irwin, 1973

Kanter, Jerome. *Management-Oriented Management Information Systems.* Englewood-Cliffs, N.J. Prentice-Hall: 1972.

Krauss, Leonard J. *Computer-Based Management Information Systems*. New York: American Management Association, 1970

Leibholz, Stephen W., and Wilson, Louis D. User's Guide to Computer Crime; Its Commission, Detection & Prevention. Radnor, Pa: Chilton Book Co., 1974.

Linde, Richard R. "Operating System Penetration." National Computer Conference Proceedings 44 (1975): 361-368.

Mair, William C.; Wood, Donald R.; Davis, Keagle W. Computer Control and Audit. 2nd ed. Altamonte Springs: Institute of Internal Auditors, 1976.

Martin, James. Security, Accuracy, and Privacy in Computer Systems. Englewood Cliffs, N.J.: Prentice-Hall, 1973.

Martin, James. Telecommunications and the Computer. 2nd ed. Englewood Cliffs, N.J.: Prentice-Hall, 1976.

Martin , James. Teleprocessing Network Organization. Englewood Cliffs, N.J.: Prentice-Hall, 1970.

Menkus, Belden. "Management Responsibilities for Safeguarding Information." Journal of Systems Management 27 (June 1976): 6-14.

Methodius, Ioannis. "Internal Controls and Auditing." Journal of Systems Management 27 (November 1976): 6-14.

Milligan, Robert H. "Management Guide to Computer Protection." Journal of Systems Management 27 (November 1976): 14-18.

Parker, Donn B. Crime By Computer. New York: Scribner & Sons, 1976.

Parker, Donn B. "Computer Security: Some Easy Things To Do." Computer Decisions 6 (January 1974): 17-18.

Porter, W. Thomas. EDP: Controls and Auditing. Belmont: Wadsworth Press, 1974.

Rosove, Perry E. Developing Computer-Based Information Systems. New York: John Wiley & Sons, 1967.

Roy, Robert H., and MacNeill, James H. Horizons For a Profession. New York: American Institute of Certified Public Accountants, 1967.

Scoma, Louis, Jr. "Data Center Security." Data Management 13 (September 1975): 19-21.

Tharp, Marvin O. "Auditor and the Systems Audit." Journal of Systems Management 27: 29-33.

U.S. National Bureau of Standards. Approaches to Privacy and Security in Computer Systems; Proceedings of a Conference Held at the National Bureau of Standards, March 4-5, 1974. National Bureau of Standards Special Publication 40, 1974.

U.S. National Bureau of Standards. Guidelines for Automatic Data Processing, Physical Security and Risk Management. Federal Information Processing Standards Publication 31, June 1974.

Van Tassel, Dennis. Computer Security Management. Englewood Cliffs, N.J.: Prentice-Hall, 1972.

Weber, Ron. "An Audit Perspective of Operating Systems Security," Journal of Accountancy 140 (September 1975): 97-103.

Weiss, Harold. "Computer Security, An Overview." Datamation 20 (January 1974): 42-47.

Wofsey, Marvin M. Management of ADP Systems. Philadelpha: Auerbach Publishers, 1973.

## PART V: SECURITY ADMINISTRATION

Chairperson: Malcolm Blake Greenlee
Citibank

Participants:

David L. Costello
Bank of America
Linwood M. Culpepper
Department of the Navy
Donald L. Eirich
U.S. General Accounting Office
Thomas Fitzgerald
Manufacturers Hanover Trust
Wallace R. McPherson, Jr., Recorder
Department of Health, Education, and Welfare

From left to right: Linwood M. Culpepper, Donald L. Eirich, Malcolm Blake Greenlee, Thomas Fitzgerald, David L. Costello, Wallace R. McPherson, Jr.

---

Note: Titles and addresses of attendees can be found in Appendix A.

## EDITORS' NOTE

A brief biography of the Session Chairperson follows:

Mr. Malcolm Blake Greenlee is an Assistant Vice President in the Comptroller's Division at Citibank. His responsibilities include the development of corporate policies and standards for data center construction, operational risk analysis, physical and communication security, and privacy. He is also responsible for assessing risk and the development and emplacement of procedures to offset new operational risks. His career began in research and teaching at Purdue University in 1956. He was associated with Johns Hopkins University from 1957 - 1968 in positions including Senior Physicist, Program Manager for satellite navigation equipment for Polaris submarines, and Program Manager at the Applied Physics Laboratory for a variety of systems. He served on the staff of the Mitre Corporation and as a faculty member at Advanced Management Research. Since joining the Citicorp organization in 1969, he has held positions as Program Manager responsible for all aspects of installing a world-wide automated payments system and Manager for all technical activities of Citicorp's subsidiary, Transaction Technology - East. He received his BS in Physics and Mathematics from Purdue, with graduate studies in Physics at Purdue and Maryland. He received his MBA in Finance and Administration from George Washington University. He has published several books and holds several patents.

The charge given to this session was:

> SECURITY ADMINISTRATION: What audit approaches and techniques can be used in an evaluation of the security administration function?

A security administration function has been established in a number of organizations to ensure the efficiency and effectiveness of the physical, procedural, and technical controls within an information processing system. Such functions have been established at various organizational levels and assigned different responsibilities. Some are staff and others line with either a centralized or decentralized concept being employed.

This session is to define the duties and responsibilities of such a function in a large organization and its most effective organizational structure. Further, the audit approaches and techniques to be used in evaluating such a function should be identified.

The following consensus report was written and reviewed by the entire group.

# Security Administration
# A Consensus Report

David L. Costello
Linwood M. Culpepper
Donald L. Eirich
Thomas Fitzgerald
M. Blake Greenlee
Wallace R. McPherson, Jr.

## 1. INTRODUCTION

### 1.1 General

Federal Information Processing Standards (FIPS) are coordinated and issued in accordance with the provisions of the Brooks Act (PL 89-306) to provide guidance for information processing systems within U.S. federal government (and related agencies) in areas such as

- safeguarding the system,
- providing for continuity of operations, and
- safeguarding the information being processed by the system.

Legal requirements for the handling of personal information are imposed by the Privacy Act of 1974. This law may be viewed as an embodiment of the desires of U.S. citizens to have certain prudent measures put in place to safeguard their implicit right-to-privacy. Organizations falling under purview of the Act tend to be very large and decentralized. This paper describes one method of coping with compliance with these public wishes expressed by law, implementation of a Security Administration Function. The implementation described is based on standard ADP auditing requirements utilizing the technology base provided by the Federal Information Processing Standards.

Given a well defined security administration function, the audit of that function becomes a standard, compliance type review.

## 1.2 Privacy Legislation

### 1.2.1 The Privacy Act of 1974

Public Law 93-579, known as the Privacy Act of 1974, was enacted into law to protect the privacy of the collection of increasing amounts of personal information. This individual data is being aggregated in the face of increasing availability of personal information made possible by technological improvements and the data requirements of an expanding governmental structure. Agencies falling within the purview of this statute are required to establish appropriate administrative, technical and physical safeguards. Agency rules for carrying out these requirements are defined in the Privacy Act of 1974 (5 USC 552a). Implementation of these rules is being accomplished by many agencies/departments by adding management structure - at each organizational level at or above the data center user. The structure performs the Security Administration function.

### 1.2.2 Laws in Other Countries

The United States is but one of the many countries that have passed or are considering public and/or private sector privacy legislation. In particular, legislation has passed in

- Sweden
- Germany, (Federal and the State of Hesse),

and is pending in

- Norway
- Denmark, and
- France.

Implications on systems design that must be addressed because of the extra-territorial features of these laws include

- trans-border information flow
- national sovereignty issues
- liability issues for interruption of information flow in time or in anticipation of war, etc.

### 1.2.3 International Privacy Law Compatibility

The Council of Europe (with U.S. State Department and the Office of Telecommunications Policy) has begun an effort to harmonize requirements of conflicting laws. It is hoped that this harmonization by treaty may occur in the not-too-distant future to alleviate the systems implications in the present (and pending) environment.

While the security administration function is implicit in many foreign laws (as in "1974"), the German law explicitly requires that a "Federal agent for the Safeguarding of Data" be appointed and provided staff to organize, manage, carry out and report on security administration. Private sector firms must have a similar structure. Because of the similar requirements of the German Law and the Privacy Act of 1974 and the clarity of definition of the function, duties, etc, of the "agent" within that law, a precis of the duties of the "agent" is attached.

### 1.3 Organization of this Report

This report is organized in three chapters and one appendix.

Following this Introduction chapter, Chapter 2 (Security Administration) discusses the planning, management control, ADP security duties and functions of the security administrator. Chapter 3 (Auditing the Security Administration Function) recommends the organizational requirements for the audit function and the audit approach to be used.

The appendix contains a precis of some pertinent requirements of the Federal German privacy law.

## 2. SECURITY ADMINISTRATION PROGRAM

### 2.1 Introduction

The concerns expressed in Chapter I have given rise to the need for the organization function of Security Administration in Federal Agencies (This may be relatively new for many Agencies).

While Security Administration includes the traditional concerns for data integrity and protection of the organization's information resources from modification, loss or destruction, it must also concern itself with safeguarding the information from disclosure or improper use. Thus, Security Administration should constitute an integrated program for protection of data in the organization's custody. We are here concerned with the principles of Security Administration applicable to ADP systems. In general, a separate Security Administration function may be practical only in large organizations. In smaller organizations, the function may be combined with other functions and jobs.

The session panel members believe that the responsibility for safeguarding the organization's data and information resources should be the personal responsibility of individuals having physical custody and accountability for it. Moreover, the Privacy Act of 1974 imposes a personal liability on any officer and employee, with criminal penalties, for improper and wilful disclosure. Thus, we believe that security of information is properly a line responsibility, extending up and down the chain of command. To segregate this responsibility from other custodial, processing and supervisory responsibilities, and place it solely upon a separate security administration entity, seems patently impractical except perhaps in unusual circumstances.

It follows then, that Security Administration[1] should be a staff function (independent of the DP line organization) supporting management at appropriate organizational levels and the central office. Security Administration should be responsible for developing overall policy and monitoring, on a continuing basis, the overall effectiveness of the security program.

## 2.2 Planning by Management

Planning for security administration is carried out at three levels within the organization. At the highest level, broad policy statements are developed which address such issues as:

---

[1] Note: Viewed in this context, 'Security Administration' as used throughout this paper is probably a misnomer and might better be designated Security Program Administration."

- What are the steps which must be taken prior to the approval of an ADP installation?
- How are exceptions to established policy granted?
- How is compliance with established policy determined initially and during the life of the installation?
- How is policy maintained and updated as a result of operational experience?

At an intermediate level in the organization, more detailed instructions which implement the policy are developed. These instructions address such issues as:

- What factors must be considered in performing the risk analysis for an ADP system? Of these factors, which are to be taken as input and therefore immutable and which can be taken as output?
- What are the checkpoints in the implementation of a system and what documentation must be completed at each checkpoint?
- What types of reports are required, who prepares the reports, and who receives the reports. Reports may be required for various levels of security breaches. For example, each level of breach may require a report to a different level within the organization.
- Who within the organization is responsible for each aspect of security? These aspects include personnel screening, audit trails analysis, security breach reporting, etc.

At a lower level within the organization, the actual implementation of instructions is accomplished. At this level, the functions performed include preparation of:

- a schedule of implementation of instruction, and
- estimates of the resources required for implementation.

## 2.3 Management Control

Management control consists of the exercise of those controls which are traditionally necessary to ensure that the security objectives of the organization are achieved, including:

Policy - the statements of management objectives for:

- the protection of organization interests,
- organizational data,
- ADP resources, and

the prevention of abuse of these resources, in an efficient and cost-effective manner. They should provide clear direction in such matters as:

- what information is to be protected,
- the levels of protection to be accorded,
- what officials have authority to disclose or release information and to whom, and
- disciplinary measures for violations, etc.

Such policy should generally be formulated at organizational levels above the Security Administration function or at the least, with full participation of top management. The policies will comprise the basis for the security program.

Procedures - descriptions of the processes and the instructions for carrying out management objectives. They must be sufficiently detailed for implementation, at subordinate supervisory levels, of those administrative, physical and technical security measures and controls described in the succeeding section. They should include the nature, timing and recipients of reporting and/or exceptions thereto. Procedures should not be limited to the execution of the ADP function, but should extend to the security of data and ADP resources employed by organizational users of these resources. Such procedures should be disseminated only after review and concurrence by the Security Administration staff.

Practices - such other activities that are dictated by traditional management principles including:

- adequate supervisory review or control,
- employee activity monitoring,
- quality control,
- investigation of known or suspected violations of the system, and
- initiation and enforcement of disciplinary actions.

## 2.4 ADP Security

### 2.4.1 Administrative Security

The security administration function must include the responsibility for development and maintainance of administrative safeguard standards, including:

- Security Implementation Plans based on analyses of the existing physical, technical, and administrative safeguards, and consideration of determinations by system managers of
    - the vulnerabilities of their data and resources, and
    - the protection necessary to safeguard against these vulnerabilities.

  Plans must detail the actions, resources and scheduling necessary to implement necessary additional safeguards.

- Contingency Plans that show the action to be taken whenever an error, unauthorized disclosure or violation of privacy safeguard procedures is detected. The plan must cover notification and where appropriate, recovery or corrective action.

- Disaster - Emergency Processing Plans which include the capability of protecting and recovering all personal data for which the facility has a safeguard and back-up responsibility. The plan must provide for continued compliance with all security safeguards.

- Facility Security Profile Documentation which documents in a single file:
    - procedures to be followed by all personnel and organizations working for or interfacing with the facility,
    - location and format of all security records such as logs and audit trails,
    - results of all internal and external security inspections,

- results of any risk analysis performed,
- copies of the facility security implementation plan, and
- copies of any contingency backup and disaster plans.

o Authorization Control Lists which include

- lists of persons authorized to enter the facility,
- authorized terminal users, and
- authorized terminals.

All lists must be maintained current.

o Programming Modifications, Testing And Validation Controls which require:

- restriction of data and system specifications to only those individuals who have a "need-to-know",
- procedures to control modifications which require testing before any program changes become operational,
- testing of new systems or modifications to systems using simulated test data,
- validation of functional adequacy and reliability of a system before the system is put into operation, and
- modular separation of the duties of analysts and programmers (when the staff size permits).

o Personnel Management Rules to

- establish authorities and responsibilities,
- develop security awareness and other employee involvement programs for the purpose of creating a positive operational atmosphere, and
- determine that adequate evaluation of potential staff members is performed.

The basic role of administrative safeguards is to establish those activities which are functions of human authorities, judgement and decision processes.

## 2.4.2 Physical Security Administration

### 2.4.2.1 Physical Access

Controlling access to the data processing facility or its individual component resources is a basic step in providing security. It should, however, be considered as only the first level of security and represents the base upon which the other levels/forms of security build. The following considerations are necessary when creating security procedures to restrict personal access.

- Areas to be restricted: may include:
  - the overall building,
  - data processing center(s),
  - all ancillary equipment and facilities (key punch, key tape, printers, bursters, etc.),
  - remote job-input or output devices,
  - remote terminals,
  - auxilliary power, fuel or water storage areas,
  - communication cable housing or concentrator locations, etc.

- Multiple levels of restriction: A person who has a valid need to access one area of the data processing facility will not necessarily need access to all or other areas of this facility. When possible, access to the individual areas should be separated and controlled individually.

- Method of access restriction: Choices of how access is restricted may include:
  - locked doors (key or combination operated),
  - guarded doors and personal identification,
  - guarded doors with badge or pass identification,
  - electrically locked doors activated by the individual using a number code,
  - electrically locked doors activated by magnetically encoded pass or badge,

- electrically locked doors activated upon checking personal identification (signature, palm or finger print (not readily feasible), or
- combinations of two or more of the above.

When determining an access control method, it will also be necessary to consider the manner in which these devices will function from inside the controlled area--particularly in emergency situations. Devices must permit free and ready exit in time of emergency for personnel safety (as required by applicable fire/life safety laws and regulations).

### 2.4.2.2 Disaster Protection

While the data processing resources should be protected against the physical damage/loss of equipment, provision for continuity of operations must also be given priority attention. Potential occurences should be ranked by likelihood, and reasonable preventative measures should be instituted. Some of the more likely occurences are:[2]

- o loss of power (total or shortage),
- o loss of water (for some equipment, air conditioning),
- o fire,
- o flood or water damage (natural, broken piping inside or outside facility, or fire activated,
- o explosion, etc.

Various methods can be employed to minimize identified possibilities. Some alternatives available are:

- o alternate public power routing,
- o private generators (with or without electrically activated uninterruptable features).
- o private water storage facility or acquisition plans,
- o appropriately rated fire resistant materials,
- o products of combustion or heat activated fire suppression/systems (Halon, sprinklers), etc.

---

[2] See also NBS FIPS PUB 31, Guidelines for Automatic Data Processing, Physical Security and Risk Management, (June, 1974), SD Catalog Number C13.52:31.

### 2.4.2.3 Back-up Facility

In the event of a total or significant partial loss of the processing capability of the ADP facility, it will be necessary to activate either a contingency plan or the emergency processing plan (see Section 2.4.1). Physical security measures must be provided for this back-up facility as well as during the movement of necessary forms, data files, output, personnel, etc. to/from the back-up site.

### 2.4.2.4 Storage Libraries

Adequate physical storage areas must be set aside for the protection of

- tape, disk, card files/records,
- program documentation including operator run documentation and programmer/analyst design and maintenance documentation,
- various administrative security control records/plans including
    - authorization lists,
    - security profile/level documentation and,
    - emergency back-up/processing plans.

These areas must be appropriately structured to preclude access by unauthorized personnel and also to protect against disaster. These libraries should generally receive the highest degree of both access and disaster security in comparison to other ADP resources. Since many of the data files will be back-up at off-site locations, the off-site facility should receive the same or comparable level of security protection. Appropriate precautions must be taken during the movement of these files between sites.

### 2.4.2.5 Data Handling and Disposal

Certain physical security techniques may be appropriate in the handling of data within the ADP facility. If multiple security levels are employed within the facility, handling of this information should be either restricted to those areas necessary, or methods must be instituted to prevent observation as the information is moved (such as by means of sealed/locked containers/carriers/trucks).

79

Consideration should be given to readily identifying, in some physical manner, data containing restricted or personal information. This could be done by means of visible labeling, color coding of labels or reels, physically separating storage locations of such files, etc. However, it should also be remembered that such techniques also readily identify these files for improper access attempts.

It is also necessary that appropriate disposal techniques be devised for outdated files, input and/or output. When information is no longer retained, the file should be erased or destroyed such as by degausing or use of write-over procedures before re-use. Computer generated scrap material such as forms used when aligning printers or when jobs are redone should be handled in the same manner as outdated input and output. Normal means of disposal include shredding, incinerating (may produce environmental problems), compaction or mulching under established control procedures.

### 2.4.3 Technical Security

- Security System

  The security officer is responsible for the maintenance of the security system programs and all files associated with it. Requests for changes in user profiles must be originated by area management with appropriate management and security approvals. (Changes to the area security administrator profiles are made only by the security administrator.)

- Data and Files

  The security administrator is responsible for the program to protect the contents and physical safety of all files. Using the security system he must ensure that the system is adequate to protect all data.

- Program Libraries

  The Security Administrator is responsible for ensuring the accuracy of program libraries. His functions in this regard include:

- ensuring that an access control program to restrict access to all programs and any test files under his control is operational
- providing copies of programs and appropriate test data only to authorized personnel upon receipt of written requests from appropriate management personnel,
- providing a method for applying program changes and ensuring a reasonable period of parallel testing, and
- providing appropriate backup facilities for program libraries and data files to ensure continuity of processing.

o Operating System

Line ADP management is responsible for the maintenance of the operating system, and should apply "fixes" generated by hardware vendors with the approval of the system programmers. Included in this is the responsibility for maintenance and testing of changes to the system. Responsibility for the change of security control security and the stability of the operating system rests with the Security Administrator.

o Teleprocessing

The security administrator is responsible for:

- user tables and teleprocessing security (including the maintenance of security modules within the TP system), and

- backup and recovery of TP systems (including backup features (e.g., dial up), line control and investigation of security violations).

o Encryption

The security administrator is responsible for:

- maintenance of encryption algorithms where appropriate, and

- control the generation, distribution and use of keys for use with the algorithm.

### 2.4.4 Training

There are two aspects to training for the security function

- training for those who implement, maintain, and operate the system, and
- training for those who use the system.

The first group should have a more formal training curriculum coupled with an established career path in ADP security administration. A variety of subjects ranging from technical aspects of design and use of ADP hardware and software to the provisions of the Privacy Act should be taught on a regular basis.

The users of the system should be given training on the the consequences of a security violation, etc. These users should be examined periodically to ensure that they are properly trained.

### 2.4.5 A Suggested Security System for an On-line System - An Example

The security system desired for large scale on-line systems must be comprehensive enough to act as an effective buffer between the terminals and the application programs and files. The level of sophistication can be reduced as system size and complexity are reduced. However, some automated system should exist. The suggested system is comprised of three security files as follows:

- Terminal file

  This file contains all necessary information regarding current status of the terminal, including:

  - Terminal ID - a unique identifier synonymous with the specific terminal. This identifier is a hardware feature of each terminal and is contained in every message sent by the terminal.
  - User ID - a unique identifier which is inserted in this file after a successful log-on. This field is appended to the transaction message prior to logging the transaction. This assures that each message contains the identification of the sending terminal, and the person sending the message.
  - Terminal status - this field contains the status of the terminal.

    - --dormant - terminal has not as yet logged on
    - --log-on in process - log-on message received but password not verified
    - --active - log-on successfully completed and user ID field updated
    - --violation - security violation attempt discovered. Terminal is logged off until investigation is completed.

  - Violation counter - this field contains the number of unsuccessful (invalid) attempts to enter either an erroneous password or an erroneous transaction type. If this counter equals some preset number, say 3, the terminal status is set to "violation."
  - Time of last transaction - if the terminal does not require log-on for each transaction this field contains the time of last transaction for an "idle" check. If the elapsed time between messages is greater than a preset idle time, the terminal status is set to dormant and a log-on is required to re-initialize the terminal.

o User profile

This file contains all information pertaining to a terminal operator, including:

  - User ID which is a unique identifier synonymous with a specific individual. This field is most commonly the employee number of the terminal operator.
  - Password which is a unique code which is entered by the terminal operator which identifies the terminal operator to the system. This data is entered by the operator in a 'print inhibit' mode. (This means the password does not display on the terminal.) After validation, the terminal status is set to "active." Note that there may be more than one level of password control.
  - Transaction codes are a set of codes which identify those transactions and application module names which the terminal operator is cleared to perform. After a successful log-on, the security system examines these fields to determine if a specific transaction code is authorized. Upon a successful match the application program module is called and control passes to the application module. If a successful match is not found the violation counter is incremented by one and the transaction is rejected.

- Transaction file

  In more complex systems the transaction file can be used in conjunction with the user profile as described below:

  - Transaction ID is a unique code used as the key for this file. It is entered by the terminal operator.
  - Sub-code is a field that can be used further to restrict access to particular data files, based on the format, within the file. If the file is broken into smaller units this field can indicate which of the units can be accessed by a particular terminal and/or operator.
  - File ID is a field which contains the identification of the master file and the specific functions which may be performed by specific transaction types against the file.

- Audit Trails

  Generally, audit trails should be employed so that Security Administration can monitor data and the system security features regulating data integrity. They can be designed to provide a variety of features to meet unique requirements for the level of security determined to be appropriate and reasonable for the perceived threats in a particular organization or activity. In general, they should be designed to record who had access to what data. Dependent upon the level of detail desired, they can identify such things as the file, the record or even the data element accessed and what transactions were performed.

The function of the Security System is to act as a buffer, reduce the probability of an accidental violation and raise the level of expertise needed to commit a deliberate violation. The system relies upon a designated security officer in each area. All violations are logged to a violations log which must be reviewed by a security officer daily and on a special log for review by the security administrator. This officer should also have an on-line hard copy terminal which notifies him, immediately, of each particular multiple violation. He should then be required to visit the terminal identified and determine the reason for the violation. The officer must reset the terminal using his special security code to permit the terminal to function again. In addition he should be required to submit a report concerning the violation to the individual responsible for security administration.

## 3. AUDITING THE SECURITY ADMINISTRATION FUNCTION

### 3.1 Organizational Requirements

The following two organization considerations are necessary when establishing a program to audit the Security Administration function.

- The Audit function should be independent of the Security Administration function.
- The Audit function may be distributed but staff audit members must report either directly to the agency head or through the head of audit to the agency head.

### 3.2 The Audit Process

The audit of the Security Administration function is simply a compliance audit. The auditor's task is to ensure that the stated policies are being followed and independently to report his opinion.

The auditor may find varying standards and procedures within the organization due to differences in size, processing environment, delegation of responsibilities, etc. Because of this, the auditor must construct or align/extract an audit program which is appropriate for accomplishing the corresponding Security Administration function. At all levels, the audit program should accomplish the following, independently of the Security Administration function.

- The auditor should appraise the policies and standards initiated in establishing the Security Administration function. The policies and standards should be:
  - comprehensive,
  - documented,
  - known and understood, and
  - complied with.
- The audit program should evaluate the degree of compliance with established control procedures and review and appraise new procedures being contemplated using generally accepted auditing standards and techniques.
- The auditor should independently verify other key control points/procedures within the Security Administration function.
- The auditor should identify any need for added controls which would make the Security Administration function more effective.

- The auditor must report findings and opinions to designated management.

The specific procedures and controls to be reviewed by Auditing will result from procedures adopted such as those suggested by Section 2.0 and the specific delegation of responsibility.

# APPENDIX

## SOME FEATURES OF THE FEDERAL GERMAN PRIVACY LAW

### 1. PUBLIC SECTOR DATA SECURITY ADMINISTRATION--ORGANIZATION

### 1.1 The Office of the Federal Agent

A Federal agent must be appointed for the safeguarding of data. The agent

- has a term of office of five years,
- is an independent office reporting to highest level of government, installed at the office of the Federal Minister of the Interior and under his service supervisory authority,
- has staff and support, and
- has his legal status precisely defined.

### 1.2 Duties of the Federal Agent

The duties of the Federal Agent include

- verifying compliance with law,
- making recommendations,
- issuing reports,
- requesting/demanding aid from other agencies,
- having 24 hour register of data banks storing personal data (public record), and
- processing/hearing appeals.

### 2. PRIVATE SECTOR DATA SECURITY ADMINISTRATION

### 2.1 Requirements for Corporate/Association Data Security Agents

A data security agent must be appointed by any person/corporation/association "who processes personal data automatically and thereby as a rule employs at least five persons on a permanent basis."

Requirements for the agent include:

- must be appointed in writing,

- o must be competent to fulfill his duties,
- o may not be put to disadvantage because of accomplishing his duties,
- o is not subject to outside direction, and
- o may appoint/employ supporting staff.

## 2.2 Duties of the Corporate/Association Data Security Agent

Duties of the Data Security Agent include:

- o assuring compliance with the law,
- o seeking assistance of governmental supervisory authorities when needed and without need for corporate/business approval,
- o keeping records on the
  - nature of stored data,
  - its purpose,
  - persons requiring access, and
  - the nature of the ADP equipment in use,
- o supervising "proper" application of the programs processing personal data,
- o training of other employees as to their responsibilities under the law, and
- o acting as a consultant to persons processing personal data.

## 3. CONTROLS REQUIRED TO SAFEGUARD DATA

Controls specifically required by the law include:

- o Access Control
  - prohibit unauthorized access to the installation (equipment), and
  - limit access to data to those having a need to know
- o Storage Control

  prohibit

  - unauthorized input to storage,
  - acquisition of data from storage
  - alteration/cancellation of stored data

- Use Control
  - prevent use of the data system by unauthorized persons (includes remote access use control)
- Transmittal Control
  - guarantee that only authorized recipients may be sent personal information via automated installations (authentication)
- Input Control

  Maintain the capability to ascertain
  - what personal data,
  - at what time, and
  - by whom was entered in the system.
- Supervisory Control
  - Supervision of instruction: authorization to process personal data
  - Supervision of transmission of personal data so that it cannot be
    - --read
    - --altered, or
    - --cancelled without supervision
  - Supervision of the organization/internal structures or boards of the company to assure that data is properly safeguarded.

## PART VI: AUDIT CONSIDERATIONS IN VARIOUS SYSTEM ENVIRONMENTS

Chairperson: Carl Hammer
Sperry UNIVAC

Participants:

- Sheila Brand, Recorder
  - Social Security Administration
- P. J. Corum
  - Bank of Montreal
- Ike Dent
  - Credit Bureau Inc. of Georgia
- Peter D. Gross
  - Computer Sciences Corporation
- Thomas L. Hamilton
  - Eastman Kodak Company
- James F. Morgan
  - GE Information Service
- Gerald J. Popek
  - University of California, L. A.
- Stephen T. Walker
  - Defense Advanced Research Project Agency
- Ronald L. Winkler
  - Sutherland, Asbill & Brennan

From left to right: Gerald J. Popek, Peter D. Gross, Carl Hammer, Ronald L. Winkler, Ike Dent, Sheila Brand, Thomas L. Hamilton, James F. Morgan, Stephen T. Walker, (P. J. Corum, absent).

---

Note: Titles and addresses of attendees can be found in Appendix A.

## EDITORS' NOTE

A brief biography of the Session Chairperson follows:

Dr. Carl Hammer is Director, Computer Sciences, at Sperry Univac as well as Adjunct Professor at the American University and a Visiting Professor at the Industrial College of the Armed Forces, both in Washington DC. His previous professional affiliation included responsibility for the initial design of the Minute Man Communications System for Radio Corporation of America, and positions as Director of the Univac European Computer Center at Frankfurt am Main in Germany , Senior Staff Engineer in the Computer Department of the Franklin Institute in Philadelphia, and teacher at Columbia University and Hunter College in New York City. He is Director of the American Federation of Information Processing Societies (AFIPS), was Science and Technology Program Chairman for their first National Computer Conference (NCC) in 1973, and Chairman of the entire 1976 NCC. He is a past Chairman of the Washington Chapter of the Association of Computing Machinery (ACM) and a Past President of the American Society for Cybernetics. By appointment of the Executive Office of the President, he is a member of the National Defense Executive Reserve. He is also a member of the New York Academy of Sciences, AAAS, IEEE, Research Society of America, and the Association of Computer Programmers and Analysts. Born in Chicago, IL, he received his degrees in Mathematical Statistics from the University of Munich (Diploma and Ph.D.).

The charge given to this session was:

> AUDIT CONSIDERATIONS IN VARIOUS SYSTEM ENVIRONMENTS: What are the considerations to be given to the audit of computer security in various system environments, such as (a) distributed processing, (b) dedicated systems, (c) time-sharing, (d) multi-processing, (e) mini/micro computers, etc.

Computer security is generally considered a function of the environment in which the system operates. A dedicated system operating in a batch mode within a benign environment has altogether different security requirements from a shared automatic resource balancing computer network.

This session will address the various system environments and identify the major aspects of each that the auditor must consider in conducting an evaluation of computer security.

The consensus report that follows was developed, written and reviewed by the entire membership of this session.

# 1. INTRODUCTION

During the two months preceding the Workshop, working papers and position statements were solicited and received. Relevant literature references were collected and disseminated. This documentation was reviewed with the members of the team during the first working session on Tuesday morning, 22 March. The team also began to develop an in-depth interpretation of its charge through unstructured and far-ranging discussion.

A structured, top-down approach to the problem was initiated toward the end of our first working day and work continued along this course during the second working session on Wednesday, 23 March. It culminated in four identifiable conceptual modules which are fundamental to the development of an open-ended, structured model of a computer security audit:

(i) Definition of three vital audit components, e.g., access control, accuracy, availability.

(ii) Morphology of systems and environments. Physical components, systems structure, and people - with five identifiable systems characteristics: Number of users, types of service, system organization, user access, and application mix.

(iii) Methodology, or the computer audit model, which establishes a scorecard value for each and every parametrically identified control capable of being audited.

(iv) Model validation through simulation, verifying empirically through four examples the power of the model as well as its completeness.

An overview of our findings is presented in this report. The Chairman takes great pleasure in acknowledging the dedicated assistance of all team members toward achieving our final goal. Their incisive thinking, capability of abstraction, and expressive writing produced the raw material for this paper. The Chairman is especially grateful to Mrs. Sheila Brand for her continued monitoring of the development of this report in addition to being a member of our team. However, he alone takes full responsibility for any errors of omission or commission which may have occurred during this editorial process.

# 2. DEFINITIONS

The principal terms relating to computer systems security used in this report are defined as follows:

Environment - The physical facilities, systems architecture, and administrative functions which constitute an ADP system to be audited.

Security Audit - An assessment of the system of controls that ensure the continuity and integrity of the environment as defined by management. An assessment of the reasonableness of these controls is achieved by examining and evaluating controls over system access, accuracy, and availability.

System Access - The ability and the means necessary to acquire, store or retrieve data; to communicate with or make use of any resource of an ADP system.

System accuracy - The state that exists when there is complete assurance that under all postulated conditions an ADP system implies (i) total logical correctness and reliability of the system, and (ii) logical correctness and completeness of the hardware and software necessary to implement protection mechanisms and to assure data integrity.

System Availability - The level or quality of service, as defined by the users, required to perform their primary functions.

## 3. METHODOLOGY

### 3.1 Audit Versus Design

The process of performing a security audit is closely related to the security determination study performed during the initial development stages of a system which is to be secured. This conclusion was reached as we attempted to develop a methodology which is based on an enumeration of all considerations applying to the audit of computer security in various system environments. We determined that specific computer related, physical and administrative environmental descriptors required close examination. They are all interrelated and not readily separated. Our end result was the enumeration of those steps to be taken first by the design team and then with slight variations by the auditors. This result should not prove too surprising if one examines the composition of an effective design team. To build cost-justifiable, comprehensive and effective security into a system at least one member of that team should have the auditor's viewpoint and hopefully be, in fact, a qualified auditor. Thus we see a two-pronged role to be played by the audit profession. First, the auditor must be an advisor to the design team providing essential inputs to the molding of the system; second, during the later, operational phase of the system the auditor must perform the traditional EDP auditor functions and reassess the effectiveness of the computer system security design.

Below, we list the steps necessary to arrive at an assessment of system security effectiveness, first for the design team and then for the audit team.

3.2 Steps the Design Team must take:

Step (1) DEFINE overall system requirements, objectives, and sensitivity.

Step (2) SPECIFY the desired environment, based on results of Step (1).

- Specification of physical parameters such as:
  - Location of system
  - Construction of "container" (building)
  - Survivability of system under disastrous conditions such as flood, fire, bombing, etc.
- Specification of system parameters such as:
  - Degree of information sharing (will there be one or multiple users)
  - Batch or interactive processing
  - Centralized or distributed data bases, processes
  - Local or remote access
  - Application mix
- Specification of administrative parameters such as:
  - Threat analysis
  - Personnel procedures
  - Organizational structure
  - Security requirements for:
    - (a) Access Control
    - (b) Accuracy
    - (c) Availability
  - Insurance
  - System development procedures

Step (3) SPECIFY control techniques that can be used to enforce the environment as defined in Step (2).

At this point, it may be helpful to point out the differences between security objectives, policy and procedures. The objectives of the imposed controls in an operational environment are regulation of access, accuracy and availability. The translation of the objective of access control into policy may take the form of personal accountability for all sensitive transactions. The translation of this policy into a procedure may take the form of logging into the system by way of a password, or manual logging into or out of a secure area.

Step (4) PERFORM a line-by-line cost/protection analysis. This is by far the most crucial step in building a set of controls to protect the system within its environment. In this step we analyze each control line item specified in Step (3) which could be employed to protect some aspect(s) of the system. The detailed cost/protection matrix will have hundreds or thousands of like items, dependent on the complexity of the system.

For each control requirement four judgments are made:

(a) Cost of implementation, development and operation of control.

(b) Effectiveness in regard to maintaining access control.

(c) Effectiveness in regard to maintaining accuracy.

(d) Effectiveness in regard to maintaining system availability.

The effectiveness judgments for (b), (c), and (d) are finally translated into (subjective) numeric values on a scale from 0 to 10, (0=non-effective, 10=super-effective). This conforms to the current state-of-the-art. However, a very desirable goal would be to devise instead an objective scale of measures of effectiveness.

For purposes of convenience, the designer may use a shorthand method of rating:

RATING = AC/A/AV

where: AC = numeric value assigned to effectiveness level of Access Control

A = numeric value assigned to effectiveness level of Accuracy

AV = numeric value assigned to effectiveness level of Availability

These ratings become part of the system documentation and are used in Step (5) and by auditors.

Step (5) PERFORM Composite Evaluation. After performing the line-by-line analysis described in Step (4) a specific subset of these controls is selected as the basis for the comprehensive set of safeguards. Management must concur that this subset provides the necessary depth, breadth and overlap of protection most cost-effectively for all aspects of the environment - physical, systems, and administrative. In other words, this is the stage at which the "risk assessment" is made and a "security" system is designed to meet the security objectives defined earlier.

Step (6) INCORPORATE the approved security controls. REASSESS this new TOTAL environment in light of the additional features inserted into the three environmental (physical, system, and administrative) parameters. If these additions do not degrade the overall system effectiveness (meeting requirements and objectives, set down in Step (1) ), the designers are ready to begin implementation. However, if after analyzing the total new system, it is found that the objectives are no longer effectively attainable, an iterative process must be initiated and the designers go back to Step (2), remolding the specifications of environment, etc., until all requirements set out in Step (1) are effectively satisfied.

## 3.3 Steps the Operational Auditor must take:

Once the system has been designed and implemented, it can go into operation. The auditor is now called upon to assess effectiveness of security controls in an operational mode. As mentioned earlier, the steps of the initial design team and those of the operational auditor are very similar. In some steps only the verb need be changed. For example, in Step (1) the designer DEFINES systems requirements while the auditor REVIEWS the stated requirements as set down by management.

Step (1) REVIEW objectives, requirements and sensitivity as documented by management for the system under audit.

Step (2) DETERMINE the nature of the environment prevailing during actual system operation, independent of the organizational descriptions. The auditor's perceptions of the physical, systems, and administrative setup may be quite different from those that were specified during the design stage.

Step (3) IDENTIFY Control Techniques used to control the environment as perceived by the auditor in Step (2).

Here we see a clear divergence from the design approach. Where the designer may have identified a large number of potential controls the auditor is confined to examining only that subset of controls which are actually implemented. The auditor makes an independent examination and may, or may not, use systems documentation as a starting point for his/her identification of the system's security components.

Step (4) PERFORM line-by-line cost/protection analysis. As in Step (3), the auditor is not concerned with all possible safeguards, but only with those implemented and properly functioning within the system, as determined by his audit. While the designer may have given values to the components of the AC/A/AV ratings on an intuitive, non-objective basis, the auditor will augment these judgmental determinations through hardware, software, and other sophisticated (where available) techniques to test the effectiveness of each component of the rating for meeting the stated security objectives.

Step (5) PERFORM a Composite Evaluation. The auditor now assesses the total effectiveness of the security system to determine whether it meets the objectives set by Management. A comparison can thus be made of the designer's rating and that found by the auditor. Since the measures used by designer and auditor are perhaps different, this will be only a qualitative, albeit incisive, comparison.

Step (6) PREPARE report of audit findings including recommendations for upgrading security where weaknesses are found, e.g., where the rating of the designer exceeds that determined through audit. It is also incumbent upon the auditor to recommend changes in overall security control requirements if the environment has changed from that assumed during the initial design or since an earlier audit.

## 4. ENVIRONMENT AND CONTROL

The key element of any systematic audit approach is a close link between the design and the audit processes while maintaining a separation of duties between designer and auditor. Care must be taken to insure that the same factors which influenced the design process are well understood and given appropriate consideration in the audit process. Two major factors must be considered: the first is the environment in which the system is to operate, and the second is the control techniques to be employed to enforce that environment. It is essential that the design process defines the environment in which the system is to operate and that the audit uses that same environmental description as a guide. If the operational environment has changed from that postulated at design time in a manner impacting security aspects of the system, this impact must be analyzed and the security control requirements must be reassessed as a part of the audit process in a similar fashion to the procedure initially used by the design team.

The approach being advocated here employs two rather sophisticated checklists and supporting material. The first checklist is used to establish, in considerable detail, the environment in which a system is to operate. In the case of a new system design, this is the list of desired system characteristics. In the case of an existing system under evaluation, this is the list of already existing system characteristics. We note that the process described in the previous chapter will work with either new systems being designed or existing systems being enhanced or merely being audited. In the audit process the statement of the environment is given. The auditor is encouraged to point out obvious inconsistencies in the environment, if he observes any, but the environmental checklist is his reference point from which he evaluates whether the control techniques specified by the designer are sufficient to enforce the given environment.

The second checklist is a description of the generic classes of control techniques which the designer may employ to enforce the environment in which his system must operate. As will be seen later, these range from physical locks and fences, through internal hardware and software access control checks, to administrative procedures. During the design process, after the system environment is established, the designer selects those measures from the control techniques checklist which he wishes to utilize to protect his system. Each of the entries in the control techniques checklist represents a segment of a continuum. Each item contains a range of measures with two related variables: the degree of protection afforded and the cost. At the low range little protection is achieved and usually cost is minimal; at the high range, a great deal of protection is achieved and the cost may be proportionately high. In the example of physical locks on doors the range might be from a simple padlock through a sophisticated electronically controlled and centrally monitored door locking system, with proportionate cost ranges. Given the sensitivity of the information contained in the system (from the environment statement) the designer must select those control techniques he wishes to employ and the appropriate position on the protection/cost scale for each chosen technique to provide in the composite the necessary measure of security control.

From a security viewpoint, there are three basic criteria in determining the environment and in evaluating the suitability of control techniques to enforce that environment: access control, accuracy, and availability. Each of these factors must be addressed in the environmental assessment, and each of the control techniques being applied must be rated against all three factors. Some control techniques will not apply to certain of these measures; for example locks do not affect the accuracy of the information but they have a significant effect on access control and on availability of the system. In the environmental statement the degree of protection needed in each of these areas must be stated and in the overall evaluation of the control techniques a rating by the designer and the auditor of each of these measures must be calculated and compared against the environmental requirements.

Many of the entries in the control techniques checklist are complementary. If one measure is taken another measure is perhaps not required. Investment made in one control technique will determine the extent of the investment needed in a complementary technique. The relationship between entries in the control techniques checklist is complex. To insure that sufficient measures have been taken to completely but not overly enforce the environment, the interactive relationship of controls within various environments must be explained in a guidelines book which should accompany the checklist (see section 5). The guidelines book will describe relative levels of effectiveness and cost of the various control techniques and will provide relative assessments of feasible tradeoffs.

The designer establishes both the environment in which the system is to operate and the appropriate control techniques. The process employed by the auditor in determining if sufficient control techniques have been applied is quite similar. The designer scans the control techniques checklist line-by-line, selecting appropriate items to be employed. Then he evaluates the achieved overall security of the system with an overall performance analysis determined by logically aggregating the selected effectiveness measures assigned to the line-by-line entries. If this overall analysis does not provide sufficient protection, or if it exceeds the constraining cost factors, then he reevaluates the control techniques or perhaps the environment itself, making such changes as necessary to achieve the security needed at a suitable cost.

The auditor, given the environment checklist, determines first that the actual operational environment is that assumed during the design stage. He then determines the control techniques which he believes appropriate to achieve this environment. He compares his control techniques checklist with that of the designer and weighs the differences so as to have a reference against which to perform his detailed analysis. He performs a line-by-line evaluation of the entries in the checklist and then an overall analysis similar to that done by the designer. Having completed the overall analysis he may go back and adjust his assessment of the individual control techniques based on a more complete understanding of the total system. The result of this audit process is an overall rating of how close the design comes to enforcing the security requirements of the operational environment. If this audit process produces a rating of sufficient protection then the system can be approved for use. If it yields an insufficient rating then the designer must go back once again to the control techniques list or to the environmental checklist and make appropriate changes to insure the necessary security of the system.

The critical element in this process is the use of the same checklist information by both the designer and the auditor. This insures a common base from which to discuss related matters. It is this common starting point that is the crucial element of our methodology. The selection of elements from the control technique checklist and the degree of protection afforded each element are often subjective and the designer may wish to take issue with the auditor over specific ratings the auditor has given for some of these measures. The crucial point is that all elements of the design are understood by both the designer and the auditor in a common context. This complete and common listing of measures used by both the designer and auditor is an element that has been lacking in previous audits.

## 4.1 Checklists

Both the environmental and control techniques checklists are divided into three sub-categories: Physical, system, and administrative. In the environmental checklist under the physical heading are those elements of the physical environment which materially affect security of the system. Included is the geographic location of the system, taking into account the susceptibility to natural and man-made disasters such as floods and crime, any special power or air-conditioning requirements, etc.

In the system environment list are those measures which describe the internal structuring of the system. In particular we find here those elements which affect the requirement to rely on internal hardware/software measures to enforce the security of the system. Under administrative measures are included such factors as the sensitivity and correctness of the information contained in the system, postulated threats to the system, etc.

The system environment comprises five physical and logical components or main categories:

1. Degree of Sharing: Single vs. multiple user(s)
2. Type of Service: Batch vs. Interactive
3. Organization: Centralized vs. Distributed
4. User Access: Local vs. Remote
5. Application: Dedicated vs. Multi-purpose

The control techniques checklist is comprised of the same three categories: physical, system and administrative. The physical controls include the traditional "put the system in a vault" measures, including perimeter control, hazard protection and backup mechanisms. System controls include hardware/software access control techniques, program integrity measures, audit trail techniques and failure response procedures. Administrative control techniques include what are commonly referred to as Change Control Procedures. Each of the control techniques must be evaluated against each of the access control, accuracy, and availability factors and an overall score must be arrived at for each of those factors.

### 4.2 Guideline Book

A critical element in the methodology described here is the background material which supports the checklist. This guideline will be composed of two sections. The first has a line-by-line description of the elements of the environmental and the control techniques checklists; in the latter case the range of protection cost of each of the entries is given. The environmental checklist must be cross-referenced against the control techniques checklist so as to insure that if a particular element of the environment is specified, some range of control techniques can be applied.

Another element of the guideline book must deal with the interrelationship between control techniques. From it both the designer and the auditor must be able to determine that if a certain control technique is employed, this may very well negate the need for another control technique. An obvious example is that if sufficient physical control measures are taken and if all personnel associated with the system have equal access to the information on the system then reliance on internal software access control techniques may be significantly relaxed. This evaluation guideline is highly sensitive to the state of technology and will need to be updated frequently. Specifically, the relationship between cost and effectiveness of a particular form of protection will need to be revised frequently, and new techniques will have to be introduced as they are developed and become viable.

This overall methodology is a systematic approach to the problem of auditing a computer security installation. The approach is systematic since the designer and the auditor as well work from a complete list of both the environment in which the system is to operate and the control techniques which are to be employed to enforce that environment. By working from common lists, the designer and the auditor can more readily communicate differences in their evaluation and reconcile their evaluations.

A number of such checklists are already in existence; they can be used to form the basis of the environment and control techniques checklists. The establishment of a complete and accurate guidebook giving both the line-by-line descriptions and the element interrelationships is a crucial element of this overall methodology yet to be accomplished. For example, see: Data Processing Security Evaluation Guidelines; Peat, Marwick, and Mitchell & Co., Certified Public Accountants; 345 Park Avenue, New York NY 10022.

## 5. GUIDELINES

In section 3 we discussed audit methodology and the sequence of steps which an auditor will follow, preparatory to executing his audit function addressed here. Therefore, the purpose of this section is to discuss those considerations which comprise the "ideal" against which the auditor compares and measures data security in various system environments.

The "ideals" are derived from several sources, including: (1) Information and experience which the auditor brings to his task, and (2) Information and observations gathered by the auditor in his effort to more fully understand the system to be audited.

In this section we will not attempt to create an actual book on audit guidelines. Several such reference materials exist already. Furthermore, the brief time available for this workshop precludes any such (exhaustive) effort. However, as shown in the charts appearing in the Appendix, we have attempted to identify significant categories of control techniques, as well as (in selected instances) some more specific security measures. While the various options within the control technique categories can be expanded upon by utilizing materials contained in reference works (and from the auditor's own knowledge and experience) we have chosen categories of control techniques which reflect major security options (in a general sense) that also provide an opportunity for analysis of the differences among selected system environment examples.

Our discussions indicated clearly that there are, theoretically speaking, many possible system environments, resulting from a combination of physical, administrative, and systems design points of view. In order to respond to the mandate given this group, we chose four sample systems which differed significantly from one another, representing four of the most prevalent kinds of systems existent in today's computer processing environment.

The description of the "environment" for each of the four sample systems is given in the Appendix; the method by which the constituent elements of an "environment" were ascertained, was discussed in section 4 on environment and control. The kinds of control techniques which we have assigned as possible protective measures with respect to the four sample systems were briefly explained in that same section.

However, our group took the further step of assigning subjective numerical scale values (ranging from a low of 0 to a high of 10) to the three categories of control techniques. Our choice for these values was derived from the group's consensus of whether such control techniques would be important with respect to the sample system. This importance factor was considered for each of the three basic categories of protection which our definition of "security audit" gave their AAA (AC/A/AV) rating: 1. Access control, 2. Accuracy, and 3. Availability.

It is clear that there are certain general audit considerations which an auditor will utilize in determining the vulnerability of a given system. These are the experience items which the auditor must bring with him, to successfully complete the assigned task.

In the Appendix, therefore, we considered only some specific aspects of the four sample systems. We highlighted those that affect security considerations in a way that distinguished one system from another. Obviously, in a complete audit of security, one would expect an auditor to perform a much more comprehensive analysis. But we assumed that the purpose of the mandate given to our group was to focus upon specific problem areas in different system environments to which an auditor should pay particular attention. The more general case, as the proverbial textbooks explain, will be left as an exercise for the reader.

## 6. CONCLUSIONS

William C. Mair, co-author of Computer Control and Audit, recently observed that "DP Auditors are not and cannot be policemen." He stated that the primary responsibility of the DP Auditor is to act as an advisor to management, to emphasize the need for standards which must be properly documented and communicated. Standards serve as the foundation on which everything else is built: they provide direction, predictability and criteria for evaluation. Through these standards the auditors establish systems controls which in turn help reduce adverse effects encountered in a basically hostile environment. In fact, the auditor is part of these controls.

Areas of vulnerability must be exposed to reduce risks to acceptable levels. The dangers confronting EDP systems include, above all, erroneous management decisions; but also embezzlement and fraud, loss or destruction of assets, excessive costs and deficient revenues. Their impact can be severe, leading to competitive disadvantage, statutory sanctions, even to economic, political, and military disasters.

We must not ever underestimate the power, ingenuity and perseverance of the "enemy". As we relate development of controls to potential exposures, we must follow a rather simple-minded approach: if we can think of it, someone else can also. Thus the auditor must be ingenious about gathering basic and detailed information; about evaluating the system's strengths and weaknesses; and about testing its design and performance. He must review all of its components individually and collectively according to a structured model specifically designed for that purpose .

A definitive, open-ended model has been developed to structure both the initial internal design and the follow-up (external) computer security audits in various system environments. The model is predicated on the notion that for a system to be viable within a well-defined (and definable) environment, we must certainly maintain control over access to the system, must provide accurate services and must assure the timely availability of these services to the users.

In making the audit, we assume the availability of standard guidelines for rating all identifiable system line items with regard to their contribution to access control, accuracy, and availability. A global measure of security audit can thus be derived from the line items' individual, local ratings. A number of algorithms have been suggested for converting the aggregate "local" into "global" ratings, but it appears as if only absolute and total compliance with the design specification ratings will be acceptable in the security environment.

In summary, we find that people are the critical element in all computer security audits. To attain perfect security, therefore, we are left with an obvious choice: Either we abolish computers or we abolish people...

# APPENDIX: FOUR EXAMPLES

To determine the effectiveness of the proposed methodology, four representative types of systems covering various facets of the system environment were partially analyzed. The results of the analyses are discussed here.

## 1. SYSTEM SELECTION

The four system types selected reflect at least one example of each category in the wide spectrum of possible system environments:

1 - College computing center
2 - Airlines reservation system
3 - Electronic funds transfer system
4 - Welfare check disbursement system

The objectives/requirements of each system were discussed and pertinent constraints and assumptions were indicated. As the analysis proceeded, further assumptions about the system objectives or constraints were required for clarification. For example, it was assumed that the college computing center was used strictly for training purposes and for nonsensitive research. No sensitive information (e.g. grades, payroll, etc.) and no critical applications (e.g. class scheduling) would be placed on the system. Similarly, it was assumed that the airlines reservations system had extremely high availability requirements but could tolerate errors to some "reasonable" extent. The electronic funds transfer system was assumed to be a network of individual processors located in separate financial institutions, retail outlets, etc. linked via cryptographically protected lines to provide for the transfer of funds between sites as one of their functions. The welfare check disbursement system was considered typical of large single-function dedicated funds disbursement systems much like a dedicated system to prepare corporate payrolls. It was assumed that inputs arrived on magnetic tape and one run per month was made to prepare the checks.

## 2. DETERMINATION OF ENVIRONMENT

### 2.1 Physical

Two factors were selected as typical of physical environmental concerns which must be covered by the audit: location and survivability requirements of the system.

### 2.2 Systems

The systems environment was the main focus of this workshop.

The five systems aspects to be considered are:

- . Degree of sharing (single or multiple user)
- . Type of service (batch or interactive)
- . System organization (centralized or distributed)
- . User access (local or remote)
- . Applications mix (single-dedicated or multiple)

As indicated above, the four chosen systems together call upon each system environment aspect at least once.

### 2.3 Administrative

Two representative areas of administrative environmental factors were considered here: the sensitivity of the system and the postulated threats to the system.

After we selected the factors for analysis, the workshop members collectively discussed them and determined the corresponding implications for each of the four systems. Obviously, in an actual audit, many more environmental factors need be considered. Typically, appropriate elements will be selected for consideration from an exhaustive enumeration of security related factors.

## 3. IDENTIFICATION OF CONTROL TECHNIQUES

After the sample environmental factors had been established for each system, a representative sample of control techniques was developed by group consensus. Again, this work would typically be done with the help of an exhaustive list. Several techniques for each category (physical, systems, and administrative) were selected for evaluation.

### 3.1 Physical

- . Perimeter controls - this would be a composite (in this example) based on both people and "things". Various "layers" of perimeter controls would be considered (site, building, room, wall thickness, doors, locks, enclosure, etc.) and various aspects (ducting, filter, fire protections, air conditioning, T.V. monitors, guard forces, etc.)

- . Backup site - locations, security, availability, etc.

- . Disposal controls - control of output, shredding, etc.

- . Communications protection - link-by-link encryption, shielded conduits, etc.

3.2 Systems

- Internal access controls - hardware/software controls for identification/authentication, access authorization, enforcement methods, etc.
- Program integrity measures - controls on self-checking, correctness, reliability, etc.
- Error detection/correction - cyclic redundancy checks, redundancy, monitors, self-testing, etc.
- Audit trails
- Failure response - sotware and hardware
- Communications - end-to-end encryption methods

3.3 Administrative

- Perimeter access procedures
- Maintenance Procedures - software and hardware
- Backup procedures - off line and on line
- Personnel procedures - training, indoctrination, bonding, etc.
- Development procedures - standards, configuration management, certification, etc.

## 4. CONTROL ANALYSIS

Once the sample control techniques were enumerated, each system was evaluated on a scale from 0 (completely lacking) to 10 (maximum) against each control. Three criteria were used for each evaluation - the relative degree to which the control in that environment provided protection with respect to:

Access control to system
Accuracy of system
Availability of system

All members of the workshop participated in the discussion of each item and an overall consensus was used to arrive at the results shown. Some results reflect our impressions of actual systems whereas others reflect possible "design objectives". The following figures show the results of our sample analyses.

## 5. COMPOSITE EVALUATION

The next step would be to derive an overall composite rating for the degree to which the system provides protection with respect to availability, accuracy and access control; and to compare that with the security objectives determined by the system manager. This comparison must include analyses of tradeoffs between the various controls (i.e. good physical controls may permit relaxed systems controls or vice versa). It must also evaluate the "weakest link in the chain." A satisfactory technique for doing this must yet be developed.

One suggested approach would be to prepare parametric "ranges" or "maximum" values for each control technique line item as a function of a specific system environment under evaluation. These critical values could then be aggregated by subsystems to yield critical parameters for their assessment. For example, an acceptable critical value for a subsystem may be defined as the highest numerical parameter selected from the entire set of parameters which make up the line items for this subsystem. Conceptually, we can continue this process of aggregation hierarchically until all microscopic levels of control adequacy on the (lowest) line item level have been translated into macroscopic parameters on higher subsystem levels. It is perfectly conceivable, even at this very preliminary stage of the investigation, that a "standard" scale for system security may eventually evolve from the crude beginnings postulated here.

EXAMPLE NO. 1

General Purpose Multiuser Programming System (e.g., College Computing Center)

| | ENVIRONMENT | CONTROLS | RATINGS* |
|---|---|---|---|
| PHYSICAL | LOCATION: College Campus | PERIMETER CONTROLS | 2 / - / 2 |
| | SURVIVABILITY: Low | BACKUP SITES | - / 0 / 0 |
| | | DISPOSAL CONTROLS | 0 / - / - |
| | | COMMUNICATIONS PROTECTION | 0 / - / 0 |
| SYSTEMS | DEGREE OF SHARING: Multiuser | INTERNAL ACCESS CONTROLS | 2 / - / - |
| | TYPE OF SERVICE: Interactive | PROGRAM INTEGRITY MEASURES | - / 0 / - |
| | SYSTEM ORGANIZATION: Centralized | ERROR DETECTION/CORRECTION | - / 0 / - |
| | USER ACCESS: Remote | AUDIT TRAILS | 0 / 0 / - |
| | APPLICATIONS MIX: Multiple | FAILURE RESPONSE | - / 4 / 4 |
| | | COMMUNICATIONS PROTECTION | 0 / - / 0 |
| ADMINISTRATIVE | TYPE: Non-sensitive | PERIMETER ACCESS PROCEDURES | 2 / - / 2 |
| | THREATS: Denial of Service | MAINTENANCE ACCESS PROCEDURES | 2 / 2 / 4 |
| | Theft of Service | BACKUP PROCEDURES | - / - / 0 |
| | Spoofing | PERSONNEL PROCEDURES | 1 / 1 / 1 |
| | Local | DEVELOPMENT PROCEDURES | 2 / 2 / 4 |

* Note: ACCESS CONTROL / ACCURACY / AVAILABILITY

EXAMPLE NO. 2

Dedicated Data Base Management System (e.g., Airline Reservations)

| | ENVIRONMENT | CONTROLS | RATINGS* |
|---|---|---|---|
| PHYSICAL | LOCATION: Multiple<br>SURVIVABILITY: High<br>SPECIAL: Dial-In Access | PERIMETER CONTROLS<br>BACKUP SITES<br>DISPOSAL CONTROLS<br>COMMUNICATIONS PROTECTION | 5 / - / 5<br>- / 3 / 7<br>4 / - / -<br>0 / - / 6 |
| SYSTEMS | DEGREE OF SHARING: Multiuser<br>TYPE OF SERVICE: Interactive<br>SYSTEM ORGANIZATION: Distributed<br>USER ACCESS: Remote<br>APPLICATIONS MIX: Dedicated | INTERNAL ACCESS CONTROLS<br>PROGRAM INTEGRITY MEASURES<br>ERROR DETECTION/CORRECTION<br>AUDIT TRAILS<br>FAILURE RESPONSE<br>COMMUNICATIONS PROTECTION | 7 / - / 4<br>- / 7 / -<br>- / 5 / -<br>1 / 6 / -<br>- / 4 / 8<br>0 / - / 0 |
| ADMINISTRATIVE | TYPE: Sensitive<br>THREATS: Denial of Service<br>Unauthorized Disclosure of Data<br>Remote | PERIMETER ACCESS PROCEDURES<br>MAINTENANCE ACCESS PROCEDURES<br>BACKUP PROCEDURES<br>PERSONNEL PROCEDURES<br>DEVELOPMENT PROCEDURES | 4 / - / 4<br>6 / 6 / 8<br>- / - / 8<br>2 / 8 / 5<br>4 / 7 / 9 |

*Note: ACCESS CONTROL / ACCURACY / AVAILABILITY

## EXAMPLE NO. 3

## Distributed Multiuser Remote Access (e.g., EFTS)

| | ENVIRONMENT | CONTROLS | RATINGS* |
|---|---|---|---|
| PHYSICAL | LOCATION: Multiple | PERIMETER CONTROLS | 6 / - / 7 |
| | SURVIVABILITY: High | BACKUP SITES | 6 / 3 / 6 |
| | SPECIAL: Encrypted Communication | DISPOSAL CONTROLS | 5 / - / - |
| | | COMMUNICATIONS PROTECTION | 9 / - / 7 |
| SYSTEMS | DEGREE OF SHARING: Multiuser | INTERNAL ACCESS CONTROLS | 9 / - / 5 |
| | TYPE OF SERVICE: Interactive | PROGRAM INTEGRITY MEASURES | - / 8 / - |
| | SYSTEM ORGANIZATION: Distributed | ERROR DETECTION/CORRECTION | - / 8 / - |
| | USER ACCESS: Remote | AUDIT TRAILS | 8 / 8 / - |
| | APPLICATIONS MIX: Multiple | FAILURE RESPONSE | 8 / 8 / 4 |
| | | COMMUNICATIONS PROTECTION | 8 / - / 3 |
| ADMINISTRATIVE | TYPE: Highly Sensitive | PERIMETER ACCESS PROCEDURES | 8 / - / 8 |
| | THREATS: Misuse | MAINTENANCE ACCESS PROCEDURES | 8 / 8 / 6 |
| | Denial of Service | BACKUP PROCEDURES | 6 / 3 / 7 |
| | Remote | PERSONNEL PROCEDURES | 8 / 9 / 7 |
| | | DEVELOPMENT PROCEDURES | 8 / 9 / 7 |

* Note: ACCESS CONTROL / ACCURACY / AVAILABILITY

EXAMPLE NO. 4

Dedicated Batch - Dollar Disbursement (e.g., Welfare System)

| | ENVIRONMENT | CONTROLS | RATINGS* |
|---|---|---|---|
| PHYSICAL | LOCATION: Single Site<br>SURVIVABILITY: Medium | PERIMETER CONTROLS | 4 / - / 4 |
| | | BACKUP SITES | - / - / 5 |
| | | DISPOSAL CONTROLS | 5 / - / - |
| | | COMMUNICATIONS PROTECTION | 0 / - / 0 |
| SYSTEMS | DEGREE OF SHARING: Single User<br>TYPE OF SERVICE: Batch<br>SYSTEM ORGANIZATION: Centralized<br>USER ACCESS: Local<br>APPLICATIONS MIX: Single | INTERNAL ACCESS CONTROLS | 0 / - / - |
| | | PROGRAM INTEGRITY MEASURES | - / 5 / - |
| | | ERROR DETECTION/CORRECTION | - / 8 / - |
| | | AUDIT TRAILS | 0 / 8 / - |
| | | FAILURE RESPONSE | - / 0 / 0 |
| | | COMMUNICATIONS PROTECTION | 0 / - / 0 |
| ADMINISTRATIVE | TYPE: Sensitive<br>THREATS: Misuse<br>Local | PERIMETER ACCESS PROCEDURES | 4 / - / 4 |
| | | MAINTENANCE ACCESS PROCEDURES | 3 / 5 / 3 |
| | | BACKUP PROCEDURES | - / - / 5 |
| | | PERSONNEL PROCEDURES | 3 / 6 / 3 |
| | | DEVELOPMENT PROCEDURES | 3 / 8 / 3 |

* Note: ACCESS CONTROL / ACCURACY / AVAILABILITY

## PART VII: ADMINISTRATIVE AND PHYSICAL CONTROLS

Chairperson: William Hugh Murray
IBM Corporation

Participants:

W. Gregory McCormack II
Western-Southern Life
Eldred Nelson
TRW Systems Group
Kenneth T. Orr
Langston, Kitch & Associates

Susan K. Reed, Recorder
National Bureau of Standards
Barry Wilkins
IBM Corporation

From left to right: Kenneth T. Orr, Susan K. Reed, Robert V. Jacobson (visiting session coordinator), William Hugh Murray, Barry Wilkins, Eldred Nelson, W. Gregory McCormack II

---

Note: Titles and addresses of attendees can be found in Appendix A.

## EDITORS' NOTE

A brief biography of the Session Chairperson follows:

Mr. William Hugh Murray is Senior Marketing Support Administrator in the Data Security Support Programs Department of IBM's Data Processing Division. He previously managed the development of the security sub-system for IBM's Advanced Administrative System. He is the author of the IBM publication "Data Security Controls and Procedures," of five IBM training videotapes on data security, and a contributor to such other IBM publications as "Considerations of Physical Security in a Computer Environment." A frequent speaker on data security topics, he has appeared on national programs of the AICPA, EDP Auditors Assoc., INFO 76, and Data Comm 77. He has appeared before SHARE and GUIDE in the U.S. and the Diebold Research Program in Europe. In 1974, he chaired the Audit Working Group of the NBS/ACM "Workshop on Controlled Accessibility in Shared Resource Computer Systems." He holds a BS in Business Administration from Louisiana State University.

---

The charge given to this session was:

> ADMINISTRATIVE AND PHYSICAL CONTROLS: What are the audit approaches and techniques for evaluation of administrative and physical controls in an ADP environment, including contingency planning, etc.

Administrative controls are defined to include both procedural and personnel security as follows: Procedural security - The management constraints, operational procedures, accountability procedures, and supplemental controls established to provide an acceptable level of protection for sensitive data. Personnel security - The procedures established to insure that all personnel who have access to any sensitive information have the required authorities as well as all appropriate clearances.

Physical controls include the use of locks, guards, badges, and similar administrative measures to control access to the computer, related equipment, and information media. Further, it includes the measures required for protection of the structures housing the computer, related equipment and their contents from damage by accident, fire, and environmental hazards.

This session is to address the audit approaches and techniques for evaluation of administrative and physical controls with emphasis on those areas that have not been subjected to extensive coverage in the literature. FIPS PUB 31 can be used as a departure point for this session.

---

This is a report of the consensus arrived at by the working group.

# REPORT OF THE WORKING GROUP ON ADMINISTRATIVE & PHYSICAL CONTROLS
## CONSENSUS REPORT

WILLIAM H. MURRAY, BARRY WILKINS

## 1. REVIEW OF THE CHARGE

The invitational workshop on audit and evaluation of computer security was convened to "develop real solutions to computer security audit problems". Since the technology is replete with "non-problems" and "psuedo problems", this working group elected to interpret the instruction to mean "real solutions to real problems".

This working group was asked to address the audit approaches and techniques for evaluation of administrative controls and the contribution of those controls to security. We were asked to place our emphasis on areas that are not already the subject of extensive coverage in the literature, and we were also invited to comment on the adequacy of the literature. In this report we will review the context or the environment in which we have attempted to address the charges, i.e., the traditional role of the auditor and its relationship to security. It was the consensus of the group that a number of problems do exist in this area and we have attempted to articulate those problems. Some of those problems are problems for the auditor and we have attempted to set forth suggestions that the auditor may find useful in responding to those problems. Other problems relate to the "state of the practice", the literature, and the direction of the technology. These must be addressed by the broader data processing community. We have attempted to identify these issues and make some broad recommendations.

## 2. THE AUDITOR AND COMPUTER SECURITY

Traditionally, the responsibilities of the auditor have included:

1. protecting the assets of the organization
2. ensuring adherance to policy
3. and ensuring the adequacy of controls and procedures

He has functioned by making tests and examinations and by reporting and recommending. His value to management has been that he provided a view that was independent of, in addition to, and complimentary to the view provided by line management. Management would thus be in a better position to act to reduce risk or to accept it.

The auditor's tests and examinations have included comparing actual conditions to standards of good practice, to policy or other expectation, and to the environment. Variances have been sorted between good and bad, material or immaterial.

In allocating his resources, the auditor has been guided by the mandate to maximize materiality, that is, he wants to devote his resources in such a way that his findings deal with the most signficiant risks to the activity.

Security has traditionally dealt with protecting mission resources, i.e., people, facilities and data, from all natural and man-made hazards. More specifically, data processing security has been concerned with protecting all of the resources associated with the DP mission, plus all data within DP custody.

It should be clear that since they are both concerned with protecting resources and assets, security and audit complement each other. Where the DP resource is significant to the organization or where data in DP custody is essential to the effective control of other signficiant resources, then it should also be clear that audit of DP security will indeed be material.

However, it follows that in order for the auditor to fulfill his role, vis-a-vis computer security, it is essential that he have a workable definition of security, an explicit statement of policy and accepted standards of good practice. As in other audits, he must have access to the function to be audited and adequate resource. He must know what tests and examinations are appropriate for the assets to be protected and the hazards to which they are subject. Finally, he must know how to allocate his limited resource in such a way as to maximize the usefulness of his findings, and he must know how to communicate those findings in such a way as to maximize management understanding and acceptance. It is the experience, finding and conclusion of the members of the working group that the auditor is encountering some problems in each of these areas.

## 3. PROBLEMS

It was the consensus of the group that sufficient problems exist in the area of our charge to justify our efforts, and that in our report we can make suggestions and recommendations that will clearly contribute to their solution.

It was suggested by one member of the group that in audits of computer security the auditor suffers with a definition of security that is binary and absolute. Such a definition may result in the conclusion that the presence of a control is always good and its absence is necessarily bad. It was the consensus of the group that, more often than not, an organization will have no explicit statement of its security policy, nor any explicit assignment of security responsibility. While in this instance the auditor may still audit to standards of good practice, he will likely consume more resource and be less effective, since the set of good practices is larger than the set of specific practices that may have been adopted by an organization.

It is the experience of the group that in reconciling to standards of good practice, the auditor is likely to encounter a variety of problems including:

1. The documentation of the standards of good practice is not adequate or useful for his purpose; e.g., "Computer Control Guidelines" [1] documents general standards of good practice, but contains very little detail in regard to security. On the other hand, "FIPS 31" [2] is very specific to security, but is intended for managers, not auditors.

2. The auditor is likely to find a wide discrepancy between actual practice and good practice. When confronted with a variance, the auditee will say, "Everyone does it that way," and he is likely to be right. Standard practice in data processing is more often a reflection of the practices that were appropriate for early data processing systems than an appropriate adaptation of traditional standards of good practice. Often, data processing management does not even accept that the same rigorous standards of good practice that are appropriate to the users are also appropriate for them. This variance between "standard" and "good" practice is particularly

remarkable in the area of system development. Even though the variance is great and the problem significant, the auditor is frequently coerced into believing that there is no better way.

It was the consensus of the group that the auditor has a difficult time achieving an effective focus for his audits of security procedures. This problem stems in part from the literature which suffers from a terminal case of "checklistitis". Like the binary definition of security, these checklists suggest that the presence of a control is always good and its absence necessarily bad. They fail to give proper weight to the value of the resources to be protected, or the consequences of their loss; the hazards to which those resources are exposed or their expected rates of occurrence; the use to which the system is put or the applications which reside upon it.

Finally, the working group concluded that the auditors' report often fails to receive the management acceptance and weight that are appropriate to its findings. In addition to some of the items noted above, a number of specific reasons for this were identified including:

1) The reports do not discuss the standards that were applied. The standards for financial audits are "generally accepted" and do not need to be explicitly set forth. However, in audits of security there are no "generally accepted" standards. Therefore, the standards that are applied and the authority for them should be explicitly referenced.

2) The reports fail to give proper weight and coverage to the level of compliance that was found. Audit reports often discuss the level of compliance found in a paragraph and then spend pages on the variances.

The working group articulated a number of suggestions which it hopes that the auditor will find useful in improving his efficiency and effectiveness.

## 4. SUGGESTIONS FOR THE AUDITOR

In response to the problems noted, the group made suggestions on audit focus and materiality, standards of practice and their documentation, reporting, and audit scope and techniques. The first three areas are treated in this chapter. Audit scope and techniques are covered in chapters five through 10.

### 4.1 Audit Focus and Materiality

In order to maximize his effectiveness, and recognizing that absolute security equals 0 productivity, the group recommended that the auditor use the concept of an "acceptable level of risk" in whatever definition of security he elects. Within this concept it is permissable to choose among protective measures rather than to employ them all. Management need not be faulted for the absence of a specific measure if its absence does not result in an unacceptable level of risk.

It was the consensus of the working group that the single most important determinant of the sensitivity of a system is the use or application to which it is being put. For that reason we recommend that a helpful perspective from which to view the security of a system is application by application. The most effective way in which to maximize materiality is to concentrate on the more sensitive applications. Figure 1 lists some of these types.

- Develops or controls other applications (e.g., program development systems, security sub-systems)
- Writes checks (e.g., payroll, accounts payable, dividends)
- Creates credits (e.g., accounts receivable)
- Controls convertible resource (e.g., inventory control)
- Controls or contains personal, proprietary or otherwise sensitive data
- Controls or contains data essential to rendering a service or continuing operation
- Other

Figure 1. Indicators of application sensitivity

In security audits, as in financial audits, the "Sutton test" is also useful for identifying material applications for audit. When asked why he robbed banks, Willie Sutton replied, "Because that's where the money is." Therefore, the Sutton test suggests that security auditors should concentrate on applications whose scope includes very high value data or are associated with high value resources.

## 4.2 Standards of Practice and Their Documentation

Five publications were cited by members of the group as being of particular value to the security auditor. These are: _Computer Control Guidelines_ [1], _Computer Audit Guidelines_ [3], _Guidelines for ADP Physical Security and Risk Management_ [2], _Data Security Controls and Procedures_ [4], and _Control Objectives_ [5].

_Computer Control Guidelines_ and _Computer Audit Guidelines_ were considered to be the most definitive and authoritative statement of the standards of good practice for data processing and the effective audit of same. They are written by auditors for auditors. They are well-structured and easy to use. While their scope is broader than security, they contain practices and tests which are appropriate to security.

_Guidelines for Physical Security and Risk Management in ADP_ was cited as the best source for standards of good practice in physical security. It also provides data on the rates of occurrence of natural events that is useful in determining whether or not a particular measure is indicated. While complete and well-written, this manual is addressed to managers. A thorough study of this manual will be required by auditors who wish to use it.

_Data Security Controls and Procedures_ was recommended as a good source for standards of good practice for limiting risk in data processing. It also treats contingency planning and systems design for security. Although it is addressed to management, it is readily useable by auditors.

Finally, _Control Objectives_ sets forth standards of good practice for data processing management. It specifically treats the standards for physical security. It has been found useful for audits of DP practice in general and operations management, including security, in particular. This publication was prepared by EDP auditors for themselves, but the auditor who is auditing security specifically may have to do some excerpting.

## 4.3 The Security Audit Report

The working group concluded that the style of the report of an audit for computer security will have a significant impact upon its effectiveness. The group suggested that the following format might be useful.

- Executive Summary
  - Purpose
  - Scope
  - Environment
  - Conclusions

- Standards applied
- Tests performed
- Compliance level
- Variances noted
- Recommendations
- Residual risk

The Executive Summary should be addressed to higher management. In addition to describing the boundaries of the audit, it should describe the key findings in such a way that the reader knows what action, if any, is indicated. In some instances, a thorough reading of the entire report will be indicated along with vigorous corrective action. In other cases, it may be adequate simply to pass the report to the auditee for his review and follow-up. The executive should not have to look beyond the summary in order to determine his action.

The balance of the report should be addressed to the auditee and his management. Most of the corrective action that will be indicated by the audit will be taken by the auditee himself. Therefore, it is to him that the report should be addressed. Proper recognition of the fact that the auditee is a legitimate, and perhaps primary, audience for the report should contribute to a style and content that is both helpful and acceptable to him.

Since there are no "generally accepted" standards of good practice in EDP security, the report should discuss the standards that were applied and employed. This action should reference all organization policy, standards, and guidelines that were used as well as any external standards that were applied. External standards should be documented or referenced. The authority for all external standards should also be noted.

In order to properly evaluate the audit findings, management must know something about the time and effort that was applied to it. The report must describe the manner in which the audit was conducted, the value of the tests performed, and the resource consumed. An audit that involved four people for four weeks deserves more credence than one that took one (1) person one (1) week. It is not adequate in a security audit to use the disclaimer "such tests as we felt appropriate".

The level and nature of compliance found must be described in detail. This is essential if management is to be able to properly evaluate the findings and recommendations. Variances are more meaningful when viewed in the light of the general level of compliance found than when viewed alone. Failure to give due weight in the report to compliance will not only detract from the ingegrity of the report, but runs the risk of detracting from its credibility and creating unnecessary resistance on the part of the auditee.

If variances and recommendations are placed in the context of this kind of report, the working group believes that they will receive the best possible acceptance.

However, the report should also include assessments of the residual risk both with and without the acceptance by management of the recommendations. If the auditor has difficulty in articulating the residual risk, then it would be well to think the recommendations through again.

## 5. TYPES OF AUDITS

### 5.1 Introduction

Described in the following chapters are five different audit approaches for reviewing data processing security. The five approaches are not mutually exclusive. However, there are five separate identifiable modules, each of which can be done as a separate audit or combined, depending on the environment to be audited. The five audit approaches to be described are:

System Development and Maintenance Practices audit
Application Review
Installation Security Review
Security Function (Data Base/Communication Environment) Review
Compromise Attempt

These audit approaches are not treated in priority sequence. The relative importance of each audit module will be determined by the DP environment to be audited. Since most audit staffs are limited in resources, it is important that adequate time is spent in the pre-audit phase profiling the DP organization or installation to be reviewed. Only with a basic understanding of the environment to be reviewed, can it be determined which modules are applicable, what the scope of the audit should be, and where major emphasis should be placed.

The areas of audit concern, the audit purpose, the audit approach (where applicable), and proposed scope with recommended tests will be described for each of the five aforementioned audit approaches.

5.2 Checklists/References

It is not the intent of this paper to provide a checklist for each of the subject audit approaches. It was determined that there are numerous references available on the various subject areas including checklists. It was the consensus of our group, however, that the best single reference is the Computer Control Guidelines and the Computer Audit Guidelines published by the Canadian Institute of Charter Accountants.

It should also be recognized that any generalized reference or checklist on the subject matter must be tailored to the environment under review. There is no global answer or guide common to everyone and equally applicable.

The purpose of this paper is to provide a uniform approach that can be supplemented by checklists and other references.

5.3 Approach

For all five of these security audits it is suggested that the approach be the best configuration of all traditional audit techniques to include emphasis on the following techniques:

Selective Protection - identify the key effort resources and concentrate the review efforts on how those resources are protected.

Test - wherever possible verify procedures and discussions through actual tests (e.g., control report reconciliations).

Interview - conduct interviews with all involved employees and management in computer operations, programming, users, security, legal, personnel, etc. This is an area to be stressed; good interviewing techniques supported by adequate follow-up testing can greatly facilitate the audit by producing more findings in a shorter period of time.

Technical Cooperatives (co-ops) - the use of team members on these audits from other organizations or locations, selected for their technical expertise, is a very effective and well-proven technique. One word of caution: the auditor should always be in charge.

These are some of the approaches and techniques that the group felt would be very effective in conducting audits of DP security.

## 6. SYSTEMS DEVELOPMENT AND MAINTENANCE PRACTICES

### 6.1 Concern

In the audit community today, there is an ongoing debate: should the auditor be involved in System Design and Development. Both sides agree: 1) that there is a valid concern from both a security and control viewpoint that the proper development of new systems and applications is important, 2) that post-implementation enhancements are difficult at best to install, and 3) that the auditor cannot ignore his responsibility in this important area.

It is necessary in many instances to build very tight security routines into a system or application. Therefore, all aspects of DP security should be considered during design. If proper security cannot be provided, then it is conceivable a project should be halted until better technology or controls are available. This is an extremely important audit. If security is not being built in during design, it will probably always be nonexistent.

This audit approach is presented as an alternative to the two extremes of the "System Design Debate" and as a minimum level of involvement on the part of internal Auditors. It is an approach where the auditor can review the system development process rather than actively participate in the content of system design. It is particularly applicable to those audit staffs that have either consciously decided not to become involved in the content of system design or because of resource constraints cannot cover all new development projects (large organizations).

It was the consensus of our group that reviewing the management process for system design is an effective way to ensure controls are built into systems on an ongoing basis and not only when the auditor is involved.

### 6.2 Purpose

The purpose of this audit is to determine if local management is in compliance with established procedures or, given the lack of defined procedures, if local management has established and implemented adequate standards and procedures to ensure that only secure systems and applications are developed. The purpose of this review is to determine that all aspects of security are discussed and that controls are implemented where necessary during the development cycle. The auditor must determine that the subject of security is actually an integral part of all decisions made during the development cycle.

### 6.3 Approach

The audit approach will be to interview local personnel and management and to actually sample current and recently completed development projects and associated documentation, to test compliance with procedures or, in the absence of such procedures, to determine if exposures exist based on judgment and generally accepted business practices for system design.

### 6.4 Scope

#### 6.4.1 Design Standards

The obvious place to start an audit of this nature is by a review of corporate and divisional design standards and a comparison of the local organization's procedures to established company standards. An important point to remember is that the auditor should recommend improvements to company standards as well as local policy when deficiencies are noted.

During this phase of the audit, the auditor will familiarize himself with the company policy and the adequacy of the local operating procedures. More often than not, a review of local operating procedures will be reflective of the actual practices. If management has not taken the time to adequately define development procedures and formally assign responsibility for security controls, it will be a rare exception to find a well controlled and secure environment or product.

The Design Standards should discuss physical, administrative and technical controls in all of the following areas which will be the subject matter of this audit:

Organizational Controls
Access Control
Phase Reviews
Testing/System Assurance
Promotion Process
Documentation
Auditor/Independent Party Involvement
Configuration Management
Emergency Procedures

The auditor should determine the adequacy of the procedures in all of the areas. The remainder of the audit will then be devoted to testing compliance to established or recommended procedures as they are implemented in the development cycle.

### 6.4.2 Organization Control

The foundation of all controls is the organization. The auditor must evaluate the organization to determine if it is conducive to good security controls and development practices. Hiring practices, separation of duties, manpower resources, skill mix and education, are all subjects that should be reviewed during this audit. In this portion of the audit, the auditor must determine that the responsibilities and duties of the using function, programming and computer operations are clearly defined and separated; that manpower has been properly allocated to key control functions; that these functions have the required technical expertise; and, that the employees are being given adequate ongoing education.

It is reasonable for the auditor to assess whether the subject of organization control is being adequately addressed during the development cycle.

### 6.4.3 Access Control

Ensuring that access to all proprietary DP resources is limited to only those employees with an absolute need is key in this audit. A lack of controls in this area will expose proprietary data to unauthorized access; enable computer frauds; possibly result in poor data integrity; and poor documentation.

Administrative and physical controls to limit access to the following DP resources should be reviewed:

Facility
Computer installation
Hardware
Programs
JCL
Data
Output reports
All DP media

The auditor should ensure that access control is being considered during system design so that additional access or other controls can be implemented during development if necessary.

The auditor must test access control procedures by reconciling actual employee accesses to DP resources to management's list of authorized personnel. The auditor must also determine if management has limited the authorized list to only those with an absolute need.

### 6.4.4 Phase Review/Project Control

A formal, detailed, and documented phase review procedure is necessary if management is to exercise effective control over system design. The phase review is a tool to provide executive management with information about status of projects. Through the phase review cycle, meaningful checkpoints are established, whereby critical issues relating to development are addressed.

Security control is one of these critical issues which is often overlooked during the phase review for a variety of reasons.

From a security viewpoint, the auditor must review the phase review process and determine if security is considered as an integral part of all development projects. There are many questions that need to be answered. For example, is the security department involved? Is the DP security coordinator involved? Is the user involved with security? Is the security system tested, etc.?

The main point that the auditor must address is that in the early stages of all development cycles a security philosophy and documented plan is developed, agreed to, and performance to the plan is monitored throughout the development cycle. There should be adequate documentation to substantiate that security was not treated lightly. Management involvement and approach should be evidenced in writing.

### 6.4.5 Testing/System Assurance

The auditor must ensure that all security controls designed into the system are extensively tested. A comprehensive test plan and documented results should be available for review. Security should be an identifiable category in the test plan.

Also, during the test cycle, security exposures may be created if proper administrative and physical controls are not put in place to control access to live data. The auditor must ensure that live data is not used except under the most extreme circumstances, and that if it is used, controls to prevent misuse are in place.

### 6.4.6 Promotion Process

The promotion process is the process of transferring a program from a test status to a production status. In a well controlled environment, computer operations will maintain ownership of all production programs, JCL and associated documentation, and the programming function will maintain control of the programs while they are in a test status. Promoting a program, therefore, generally means transferring control from the programming function to the operations function.

During this process, many effective administrative and procedural controls can be implemented to ensure security of the programs themselves, and that security is built into the programs. The following represents a partial list of controls the auditor should look for:

- Using function request/written authorization
- Programming management approval/authorization and delegation to programmer
- Operations release of programs and documentation based on authority
- Independent party review of code to detect errors and deter programmer fraud
- Separation of test and development work from production

- After promotion, documentation, programs, JCL, data, etc., controlled by operations

The promotion process is an important part of the maintenance and development cycle. Procedures and controls during this process must be reviewed.

### 6.4.7 Documentation

Auditors frequently encounter poor documentation and are advised that documentation is written for programmers and not auditors. Poor documentation results in applications and systems that are not functional, effective, or secure, and coincidentally, are not easily enhanced, are not understood and are not auditable.

While it is recognized that poor documentation is a universal problem, the auditor should not ignore it. The product of any system or application development effort must be an adequately documented solution to a problem or need. The program or code itself is only one part of the solution, but is often given the most attention because its intended audience, the machine, is the most unadaptable and unforgiving. The intended audience for the documented solution to a problem includes management, users, operations maintainers, the machine and auditors.

Auditors are an appropriate audience by definition. Therefore, auditors should be able to understand the documentation and should critique it if they are not able to understand it. The auditor should ensure documentation standards are adequate and are being adhered to and should no longer accept the traditional excuses.

The auditor must continually review and criticize the lack of adequate documentation.

### 6.4.8 Auditor/Independent Party Involvement

Sensitive programs/systems should be subject to an independent review and verification. If the auditor does not directly participate in system design, it is important that some function be designated as the independent party. The auditor must review the adequacy of independent party involvement during system design.

### 6.4.9 Configuration Management

The auditor should expect to find a management system or mechanism for controlling which versions of each component are included in any specific integration or copy of a product system. This management system should include an audit trail that is adequate to determine for any given integration or copy, which version of a component was included. Tests should be made for the presence of the system, its adequacy for the application, that it is being used as intended, and that the audit trail is present and adequate. Where indicated, the content of the audit trail should be reconciled to the content of an integration of a product system.

### 6.4.10 Emergency Procedures

Management must have the flexibility to substitute emergency procedures for normal procedures when required to respond to unusual situations. Emergency procedure will compensate for the risk associated with extra flexibility by involving additional management. Reviewing the procedures and actual practices in the event of an emergency program fix, to prevent the bypassing of established controls, is an important part of the System Development Audit.

The auditor should expect to find procedures that ensure that all emergency fixes are subjected to the same controls after, that the normal updates are subjected to prior.

## 7. APPLICATION REVIEW

### 7.1 Concern

There are important administrative, procedural and system controls that should be in place to provide for continuous security in all applications that have been implemented. Either the absence of or deficiencies in the administration of these controls may lead to exposures.

### 7.2 Purpose

An application review is a post-installation analysis of the data processing security controls and procedures that are unique to a specific application. This is in contrast to other data processing security controls and procedures that are common across all applications in a computer environment.

The purpose of this review is to ensure that the application was designed with adequate internal security controls and that these controls are being administered in a consistent manner.

## 7.3 Approach

Application reviews should be conducted by internal auditors as an integral part of all functional audits of financial and operational areas. If a functional area depends on data processing, an audit of that function must include a review of the data processing related controls.

An audit of the functional area is not complete without a review of the DP application. Both parts of the overall audit should be done simultaneously.

## 7.4 Scope

The scope of an application review will include the following eight areas as they relate to a specific application.

Input/output controls
System internal control effectiveness
Separation of duties
Sensitive program identification
User satisfaction/involvement
Report utilization
System documentation
Vital records

Not all of these areas are applicable to every application. Each area is described briefly on the following pages.

### 7.4.1 Input/Output Controls

The system or application should provide adequate controls to ensure that only what was authorized was processed and in its entirety; nothing more and nothing less. The auditor must assess the adequacy of the control techniques and determine that they are being used as appropriate.

### 7.4.2 System Internal Control Effectiveness

The auditor must evaluate and test the adequacy of internal edit and audit routines to ensure the detection or prevention of questionable or invalid situations.

The auditor must determine if adequate internal controls exist by reviewing system documentation, inputting test transactions, questioning users and reviewing exception and control reports. The key here is to test whenever possible.

### 7.4.3 Separation of Duties

It is clear that the security of any application is dependent on the proper separation of those duties normally performed by the user, programming and operations functions. For example, in an accounts payable application, the user should not program or be able to execute the application. The programmer should not be allowed to input live data or access master files. The operator should not reconcile control totals. Refer to section 8.4.2.2 for a further discussion on separation of duties.

### 7.4.4 Sensitive Program Controls

There may be a need for additional controls for programs where there is an exposure to unauthorized manipulation of program code for the purpose of misappropriating company assets. An example of an additional control would be an independent review of every changed line of coding made to the accounts payable checkwriter program. Such a review would not be necessary for other programs even within the accounts payable application. The auditor should determine the "sensitive programs" in an application and ensure they are provided with "selective protection".

### 7.4.5 User Satisfaction/Involvement

The users should be questioned during this audit to determine if they are aware of known security deficiencies that have not been adequately resolved. The auditor must determine if the user understands the system and is truly involved in changes to it.

### 7.4.6 Report Utilization

The auditor should determine, independently from programming documentation, the control reports available from the system and determine if they are used.

### 7.4.7 System Documentation

The auditor must review the adequacy of documentation and make constructive and realistic suggestions. Without adequate documentation, a system is difficult to enhance, understand, and audit. It is important that the auditors insist upon compliance to documentation standards. Refer to section 6.4.7 for a more complete discussion of documentation.

### 7.4.8 Vital Records

During this part of the audit it should be determined that the files, programs, blank forms, etc., specific to this application have been incorporated in the installation's contingency plans.

## 8. INSTALLATION SECURITY

### 8.1 Concern

There are various levels or rings (see figure 2) of security that provide a good security posture in a DP environment. A weak control in any of these areas may lead to security exposures. The specific concerns in this audit are: 1) unauthorized access or modification of data, 2) unauthorized use of data processing resources, 3) misuse of authorized resources.

### 8.2 Purpose

The purpose of this audit is to evaluate the administrative, system and physical controls in all of these areas to provide management with an assessment of the security posture of the installation or organization under review.

### 8.3 Approach

In a multi-site organization, the auditor should first select the installation or organization with the greatest exposure. During the pre-planning stage of the audit, the auditor must carefully describe the installation under review to ensure that the audit scope does not omit any significant areas and that the audit team is selected and prepared for the unique technical aspects of the installation. Whenever possible, team members possessing required DP expertise should be selected. This not only facilitates the audit, but provides a valuable training ground for DP professionals. The audit approach will be a combination of employee and management interviews, documentation reviews, and detail testing to support or disprove interview results. Interviews alone are not sufficient without substantive testing.

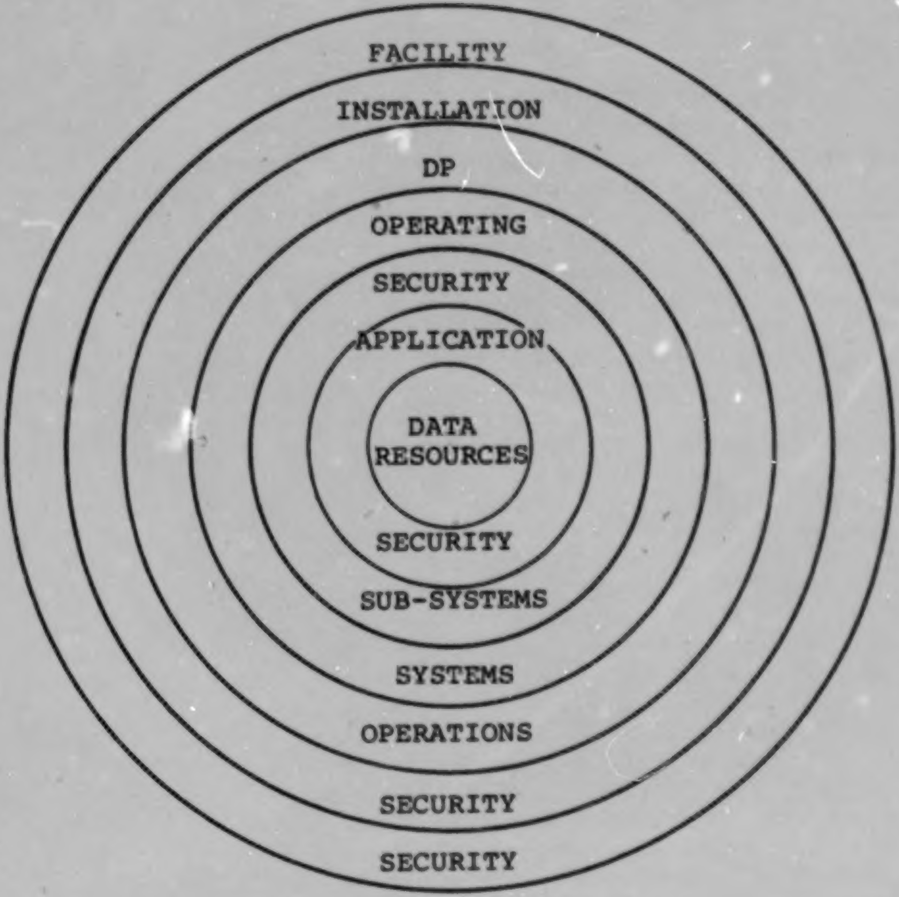


Figure 2 System Levels of Security

## 8.4 Scope

The scope of a DP installation security review in a large installation may look very complex, but it can be divided into four functional audit techniques:

1) Procedure review
2) Organizational control review
3) Access control review
4) Contingency plan review

It will be the intent of this sub-chapter to identify all auditable areas and expand on only those that are not well defined in the literature.

The scope of this audit may be further broken down as follows:

Procedure Review

Standard Operating Procedures
Self-evaluations (performance and results)

Organizational Control

Responsibilities
Separation of Duties
Termination Practices
Job Rotation
Vacation Schedules

Access Control

DP Resources

Space
Media
Equipment
Programs
Documentation
Procedures

Protection Techniques

Physical Security, site, facility,
DP installation
Classification System
Media Control
DP Operations

  - Remote Computing
  - Bulk-Data Transmission
  - Program Controls
  - Encryption

- Contingency Plan

  - Emergency Plan
  - Backup Plan
  - Recovery Plan
  - Vital Records Plan

### 8.4.1 Procedure Review

An installation security review should begin with a reconciliation of local procedures with standards and guidelines. If local procedures agree with standards and guidelines, this may be taken as evidence that the operation is consistent with accepted practice. However, the auditor must still reconcile actual practice to accepted. If local procedures do not agree with standards and guidelines, this may be an indication that local management is not devoting adequate attention to DP security.

The auditor should review the local operating procedures to determine that they are adequate and that they explicitly define responsibility. In addition, the auditor should request any management self-assessments on the subject of DP security. Concerned management may have initiated a self-review or peer review program.

### 8.4.2 Organization Control

#### 8.4.2.1 Security Responsibility Assignment

Early in the review, the auditor must make a determination that responsibility for the protection of all resources has been explicitly assigned. In addition, each employee should have been assigned responsibility for protecting resources within his ownership or custody, for noting variances and for taking appropriate and timely corrective action. Where indicated by the extent or sensitivity of resources or operations, staff responsibility for security should have been assigned.

#### 8.4.2.2 Separation of Duties

Separation of duties must exist between DP and its users, and within DP and its users. This separation should be such that: 1) no individual has access to a sensitive combination of resources, 2) no individual is in a position to fail and conceal, 3) each individual's key actions are checked upon by another individual who is only doing his assigned job and 4) each individual can be held accountable for his actions.

The auditor should examine organization charts, performance plans and such other evidence of assignment and duties as are used to determine that proper separation has been provided for. He should examine audit trails to insure that it is consistently maintained.

#### 8.4.2.3 Hiring Practices, Job Rotation, Vacation Schedules

Other organization controls such as these must also be reviewed. They are second nature to the auditor and warrant no further discussion, except to say that they are equally important in the DP environment.

### 8.4.3 Access Control

#### 8.4.3.1 DP Resources

Access control to the site or facility, the DP installation, and all DP resources must be reviewed. This includes space, media, equipment, documentation procedures, and programs. Techniques for access control to some of these resources will be discussed separately. Where appropriate, the auditor must determine, from the DP installation profile, what DP resources are critical and concentrate the review efforts there. Logs or journals of access should be in place as required to fix accountability. Tests should be made to determine that such logs or journals are routinely reconciled to expectation on a timely basis.

#### 8.4.3.2 Protection Techniques

##### 8.4.3.2.1 Physical Security, Site, Facility DP Installation

Facility and installation access control are the first two levels of protection. Only personnel whose jobs are within the facility or installation should be permitted normal access. All others should be admitted only under additional rules. The auditor must test actual access to the authorized list.

##### 8.4.3.2.2 Classification System

One important requirement for maintaining access control and other DP security controls is the adequacy of the system for identifying sensitive resources. Without a classification system for identifying the relative importance of the resources to be protected, a DP security program will not be cost effective. The auditor must test the classification system to determine that it is understood and working, that resources are being classified correctly, and that where applicable, classification termination dates are being assigned and observed.

### 8.4.3.3.3 Media Control

In order to properly safeguard media (tapes, disks, etc.), it should be labeled with its classification and each classification should have a minimum level of required controls. For example, media labeled "secret" may be inventoried semi-annually while "top secret" media may be inventoried weekly. A separate access within the DP installation should be available for storing media. An authorized access list should be available and an audit of access to media should be available. The auditor may wish to reconcile the audit trail of accesses to the authorized access list.

### 8.4.3.3.4 DP Operations - Input/Output Controls

There must be adequate controls to insure: 1) accountability, 2) that only authorized DP jobs are processed and, 3) that the resultant output is distributed to only the authorized recipients. There are numerous ways acceptable for providing these controls. Reviewing the DP operations function for the presence, adequacy and reconciliation of these controls is an integral part of this audit.

### 8.4.3.3.5 Remote Computing

Security controls in a remote computing or interactive environment are important because physical locks and keys alone may not provide for adequate accountability or deter unauthorized access. The minimum controls to be reviewed in a DP installation audit include the following:

User Identification
Data-Access Controls
Terminal Identification
System Security Administration
Audit Trails
Terminal Security
Privileged Sign-On Codes
Output Controls

(see Security Function Review, chapter 9).

### 8.4.3.3.6 Bulk Data Transmission

Data is often transmitted in bulk by mail or electronically. Depending on the data sensitivity and/or classification, certain controls may be indicated. For example, "secret data" to be forwarded by U. S. Mail may require double enveloping to conceal internal classification identification and registration with return receipt requested.

All bulk data transmission of classified data should be approved in writing and an audit trail maintained indicating date, time, sender, approver, recipient and acknowledgment as appropriate.

### 8.4.3.3.7 Encryption

Enciphering may be indicated for very sensitive data that must be passed outside the control of its owner. Only algorithms with known properties such as the Data Encryption Standard algorithm should be employed. The implementation of the algorithm should be appropriate to the application. In reviewing the use of encryption, the auditor should remember that there are costs in terms of system performance that must be considered.

The auditor must test to ensure data is encrypted where necessary and that good encryption procedures including key handling have been implemented.

### 8.4.3.3.8 Program Controls

Access controls must also be in place to protect programs, JCL and related documentation from unauthorized access. A program may be proprietary for its intrinsic value or it may be "sensitive" from the standpoint that unauthorized changes could facilitate or conceal misappropriation of company resources. In either case, it is important that programs and related JCL and documentation be protected from unauthorized access. Controls should be adequate for the integrity of the change history.

### 8.4.4 Contingency Plan

During this review the auditor must determine that the installation is prepared in the event of any natural or man-made disaster or any other happening that would severely interrupt normal business operations. The auditor should expect to find plans for detecting and limiting emergency events such as fires or intrusions (emergency plan); accomplishing critical jobs on a timely basis (backup plan); recovering mission capability (recovery plan); and a plan for identifying and protecting data vital to customer, employee, or stockholder equities, data related to national interest (vital records plan).

The key to successful contingency planning is periodic testing. It can reasonably be assumed that a contingency plan will not be effective, if it is not tested and updated annually. The area of contingencies should not be left to chance. The auditor should look for evidence that the plan has been both tested and updated.

## 9. SECURITY FUNCTION REVIEW

### 9.1 Concern

The security department or function provides for the articulation of security policy, the allocation of security resource, the definition, communication, and administration of security rules, the timely recognition of variances, and the recommendation of corrective action. It is a staff function serving all levels and functions of management. Depending on the nature and scope of the system it supports, this function may be responsible for extensive computerized data and procedures for carrying out its responsibilities. Its data may include statements of authorization, system or application access rules, and notices of variances. Its procedures may include programs for applying or maintaining access rules, or for communicating or analyzing present rules or notices of variances from them.

This staff is responsible for the implementation and operation of all security controls that are generalized across applications and operations. It may be viewed as a vendor of access control, monitoring and advisory service to applications, and as a vendor to, and customer of, operations.

The proper functioning of this department or staff, and the integrity of its data and programs, may be vital to the uniform, timely and consistent application of all security controls and procedures.

### 9.2 Purpose

The purpose of the security function review is to insure that: its facilities and organization are consistent with good practice and the needs of the installation and applications; its resources are consumed as management intends and that using departments are receiving satisfactory service; that its actions are consistent with management and using department authorization; that its audit trail is adequate to demonstrate authorization, accountability, accuracy and completeness; and that variances are dealt with on a timely basis.

This review is indicated whenever significant security functions or services are generalized across using departments or applications such as in time-sharing, data-base, or interactive environments.

## 9.3 Approach

Depending on the size of the installation or system to be audited, a review of the security function may be a module of another audit (e.g., a DP installation audit) or it may be done as a stand-alone audit. Security may be viewed as an application and audited accordingly (see Application Review, chapter 7). The same audit approaches and techniques should be used in this audit as discussed in the prior audits.

## 9.4 Scope

An outline of the scope of this audit is as follows:

General

- Responsibility Definition
- Standard Operating Procedures/Users Manuals
- Self-Reviews of DP Security
- Education
- Employee Awareness

Security Administration (Interactive)

- Administering Security Codes
- Monitoring
- Reporting
    - Violation
    - Critical Transaction Usage
- Terminal Authorization
- User Authorization
- User Termination

**Access Control**

DP Resources
    Space
    Media
    Equipment
    Documentation
    Communications

**Contingency Plans**

Emergency Plan

## 9.5 General

### 9.5.1 Responsibility

The security function is generally a staff function responsible for overseeing and monitoring DP security. The auditor must ensure that this function has been clearly defined.

The security function serves user management by administering access rules within the system. The auditor should look for adequate audit tools to ensure all administrative activity is as authorized.

### 9.5.2 Standard Operating Procedures/Users Manuals

It is the responsibility of the security function to ensure local security guidelines, operating procedures and users manuals are written and properly maintained. The auditor should review these documents, as indicated, and test for currency.

### 9.5.3 Self-Reviews or Peer Reviews

The auditor should request the results of any self-reviews or peer reviews on the subject of DP security and the corresponding action plans and progress to date. An analysis of self-review information will give the auditor a good insight into the organization and problems identified, but does not relieve him of the responsibility to complete the audit. The auditor may, and should, use the results of the self-reviews where applicable in his final report as long as the source of the information is acknowledged and the resulting comments are put in proper perspective.

### 9.5.4 Education

It may be the responsibility of the security function to both conduct tailor-made education courses for the line functions and to ensure that these functions take full advantage of all applicable security courses on DP security. Evidence of the performance of such responsibility, including class schedules, syllabus, and rosters, should be reviewed.

### 9.5.5 Employee Awareness

This is perhaps the most important aspect of the security function's job. Because the subject of DP security may be viewed as negative, the auditor must determine what the security function is doing to make it positive and to maintain employee awareness and concern. The possibilities in this area are limitless. Posters, suggestion programs, informal awards, breakfasts, luncheons, guest speakers and executive management speeches are only a few of the possible ideas. Instead of guards only noting violations, they could leave a thank you note for securing proprietary data. The content of the awareness program might point out the value of assets and the importance of the employees' role in protecting them.

In any event, this is an important area. An effective DP security program is not possible without the concern and commitment of the employees.

## 9.6 Security Administration (Interactive Environment)

Generally, in any interactive system someone, or a group, in a staff capacity has been designated the security administrator. The proper performance of the associated responsibilities is important to maintaining effective system security. The responsibilities of a security administration may include:

- Authorizing use of system resources
- Administering security codes
- Monitoring user activity
    - Violations or variances
    - Critical transaction usage
- Terminal authorization
- User authorization
- Data access control
- User security education
- Contingency plans

The auditor must test the security administrator's performance in all of these areas. The auditor should expect to find written evidence to support the proper execution of these tasks.

An area of the security administrator's responsibility that is often overlooked is user involvement. The security administrator should motivate user involvement, understanding, and perhaps most important, feedback. The security administrator should continually review user security practices.

### 9.7 Access Control

In this audit the security administrator's role in access control or the monitoring of access control must be evaluated. Refer to section 6.4.3 for more detail. The security administrator is generally responsible for advising management of any control deficiency.

### 9.8 Contingency Plan

The security administrator's role in creating, implementing, and evaluating contingency plans should be reviewed. Refer to chapter 8.4.4. The auditor should insure that proper treatment of the security function is included in all contingency plans.

### 9.9 Summary

The security administrator's job may be viewed as writing security procedures, implementing them and then reviewing compliance. Any control deficiencies noted during a security audit are a direct reflection on the security administrator's job performance, unless they had been previously noted and escalated to the right level of management for resolution.

## 10. CONTROLLED TESTS/PENETRATION STUDY

### 10.1 Concern

The purpose of this audit is to resolve fundamental and recurring problems and exposures that auditors have continually pointed out to management that have not been resolved. Because of the types of problems noted in chapter 3, it often happens that management does not pay attention to the auditor's concern. Management may have an attitude such as, "it can't happen to me".

## 10.2 Purpose

The purpose of this test is to dramatize to the executive management the need for DP security by perpetrating an unauthorized act.

## 10.3 Approach

The auditor may use his knowledge of DP control exposure, but should not use audit privilege. At the successful completion of the test, the auditor must be able to demonstrate beyond the shadow of a doubt that the compromise could have been perpetrated by another employee or an outsider. The auditor must be able to prove audit privilege was not a factor.

The chance of success for an undetected compromise should be better than 90%, since if the attempted compromise is discovered, the opposite effect of what was intended will be accomplished, not to mention embarrassment to the auditor.

Such a compromise plan should be enacted only with the concurrence of audit and executive site management. The test must be controlled to prevent the auditor from being put in a situation where he could perpetrate a real fraud without detection.

The group concluded that this is an effective, but dangerous approach that should be well controlled and carefully planned as a last resort.

It is, however, a highly effective technique, when done in a truly professional manner.

## 10.4 Scope

The scope in this situation is limited only by the individual's imagination. The following areas represent possibilities for a penetration study. Each of these potential areas will be discussed briefly on the following pages. Any penetration study is unique to the environment and must be assessed on its own merits:

1) Application programming
2) DB/DC systems
3) Information security

### 10.4.1 Application Programming

Assign an EDP auditor to application programming with the instructions to attempt to perpetrate a fraud without detection by manipulating program code. The application to be selected should present a high probability of success (e.g., payroll). This approach is equally applicable to a batch or an interactive environment.

### 10.4.2 Data Base/Data Communication Environment

Either by posing as a user or actually working in a sensitive user area, the auditor should attempt to bypass system and administrative controls in an undetected manner to misappropriate company assets. This approach generally requires expending enough time to thoroughly understand the application and surrounding controls.

### 10.4.3 Information Security

This approach is applicable where the information itself is highly proprietary (e.g., research and development environment). The purpose is to bypass controls and obtain highly proprietary company data in an undetected manner. The same approach can be used to prove the vulnerability of this data to unauthorized modification or destruction. A simple and effective application of this approach might include an auditor making after hours tours in terminal rooms looking for a password and/or a user's manual carelessly left behind. Subsequent access attempts from a remote terminal using the user's manual and sign-on password, will more than likely yield interesting results and prove the need for greater security.

The key to this approach is to obtain undetected access to important information while being unauthorized, and by not using audit privilege. Being able to demonstrate that anyone (employee or cleaner), who has access to the building, could have obtained unauthorized access to the information is key.

### 10.4.4 Summary

Unauthorized penetrations, while unorthodox, are valuable ways to demonstrate the auditor's concerns to management, when those concerns are fundamental, recurring, and are not getting management action. However, they require extensive planning, and sometimes, relatively extensive devotion of resources with no guaranteed payback. Penetration attempts are also risky and prove the auditee's rather than the auditor's case, if unsuccessful. This is not to mention the possibility of loss of creditability.

# 11. ISSUES FOR THE COMMUNITY

The working group concluded that there are at least three issues to which the data processing community must address itself in the coming years. These issues can be expected to have a significant, if uncertain effect, on the security and auditability of systems. They are the implications of technology advances, adequacy of the literature, and the state-of-the-practice of data processing.

## 11.1 Implications of Future Technology

There are several directions that are evident in the technology that can be expected to affect the security and auditability of data processing in the future. These include the increasing density and portability of media, mass storage, and distributed systems.

As the density with which we can record information on media increases, the portability of the data goes up. This means that the exposure of the data to theft or conversion will also increase. At the same time, smaller volumes (e.g., cartridges for the IBM Mass Storage System)* are being introduced. Large quantities of data can be recorded on volumes small enough to be easily secreted on a person.

This tendency is offset in part by the introduction of mass storage systems which enable us to move even larger quantities of data inside the control domain of the hardware. The effects of this will include a reduction in manual intervention with the concomitant opportunity for error, and an increase in the uniformity, consistency, and timeliness of control. However, since more and more data will be subject to a single event, data-base back-up procedures will become increasingly important.

---

*Editor's Note: Other small volume storage devices exist in the marketplace. The identification of this particular one does not imply recommendation or endorsement by the National Bureau of Standards.

Distribution of systems over geography will reduce the amount of resource subject to a single event. It can be expected to reduce communication cost and improve response time. On the other hand, it cannot be expected that management control will be as uniform or as effective over a distributed system.

Obviously, some of these technical directions are inherently positive. All can be dealt with given proper attention. It was the sentiment of the working group that management needs to be alerted to the implications and possibilities of these technology advances.

## 11.2 Adequacy of the Literature

It was the consensus of the group that the literature for auditing data processing security is adequate in the sense that everything is written down somewhere. As might be expected in a new discipline, the literature suffers from style and orientation, lack of audience sensitivity, volume, and absence of authority.

The style and orientation of the literature often obscures its content. Organization and structure is different for each source. Reference is seldom made to models or structures used in other sources. Not only does this make it difficult to relate material from separate sources, but it makes it almost impossible to test any source for completeness.

Emphasis is often placed upon examples, implementations and procedures, rather than on objectives, principles and guidelines. This places the responsibility for identifying and articulating objectives and principles on the reader. It dates the material and obscures its applicability to new media or technology.

Most of the material in this area is written for managers rather than auditors. Often this makes the material less useful to the auditor. Some material is designed to attract the largest possible audience. It can hardly be expected to serve anyone well. Even that material which is designed specifically for auditors may not say so, so that even the material which is useful and appropriate, may be difficult to find.

There is a plethora of data being published. While this may not appear at first glance to be a problem, it places upon the reader a requirement to sort the readable, useful and applicable from the other ninety percent. This process is complicated by the fact that the credentials, experience and claims to authority of the author are frequently inadequate or unknown.

The working group felt that there is a need for a single compendium produced by a reputable and authoritative institution. This reference should be developed with auditor involvement. It should stress objectives and alternative solutions. The group also saw a need for the same material to be covered several times, or at least cross-referenced, once for each of the involved audiences.

### 11.3 State-of-the-Practice

The working group was extremely critical of the state-of-the-practice in data processing. Much of what appears to be audit or security problems in data processing is in reality the institutionalization of bad practice. While this bad practice may not be serious or risky in operations, it is extremely serious in systems development.

This problem was seen by the group as a management failure rather than a technical problem. Managers are seen as controlling process and schedule while neglecting product and quality.

Today's inadequate practice is seen as resulting from tradition and inertia, from the effect of the tools, and from a perception on the part of managers that programmers are resistant to change. Today's practice is the result of the brief history of programming. Half of that history was spent in relatively slow and expensive machines that worked on one job at a time. The practice that was appropriate for those machines is inadequate for today's resource-sharing systems.

Managers appear to be reluctant to introduce new control because they fear that programmers will resist any change to the way they do their jobs. It is ironic that a technology whose success depended upon its ability to get its users to accept change, is now threatened by the reluctance of its practitioners to accept change.

The working group was unanimous in its conclusion that data processing management must move with all deliberate haste to improve the state-of-the-practice in programming application development and system development. They must implement all of the so-called "improved programming technologies". They are reminded that these techniques are in reality management tools and not programming tools. As such, they must be implemented by managers and not programmers.

The use of the new management techniques will require, and will be facilitated by the development of new tools to support programmers. These new editors, compilers, and library managers must support the role of managers in authorizing, naming, reviewing and reconciling programs. They must be restrictive and controllable as opposed to permissive and flexible.

It was suggested that programmers are not as resistant to change as their management perceives them. They are at least as flexible as their users. Like their users, they will respond and adapt to new management expectations and improved tools.

The most urgent item on the agenda of the data processing community is to learn to build auditable systems in an auditable way.

## REFERENCES

[1] Computer Control Guidelines, Toronto, Canada: Canadian Institute of Chartered Accountants, 1970.

[2] Guidelines for Automatic Data Processing Physical Security and Risk Management, U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., Federal Information Processing Standard Publication (FIPS PUB) 31, September 1974.

[3] Study Group on Computer Control and Audit Guidelines, Computer Audit Guidelines, Toronto, Canada: Canadian Institute of Chartered Accountants, 1970.

[4] Data Security Controls and Procedures (G320-5649), White Plains, New York: IBM Corporation.

[5] EDP Auditors Association, Inc., Control Objectives

# PART VIII: PROGRAM INTEGRITY

Chairperson: Clark Weissman
System Development Corporation

Participants:

Richard Canning
Canning Publications
Theodore A. Linden, Recorder
National Bureau of Standards
Don C. Lundberg
IBM Corporation
Harold J. Podell
U. S. General Accounting Office

Carl B. Spencer
Glendale Federal Savings and Loan Association
Douglas Webb
EDP AUDIT Controls
Edmund L. Burke
The Mitre Corporation

From left to right: Harold J. Podell, Carl B. Spencer, Richard Canning, Clark Weissman, Edmund L. Burke, Don C. Lundberg, Douglas Webb, Theodore A. Linden

---

Note Titles and address of attendees can be found in Appendix A.

## EDITORS' NOTE

A brief biography of the Session Chairperson follows:

Clark Weissman is Deputy Manager, Research and Development Division, and Chief Technologist with System Development Corporation. He is responsible for the corporation's Independent Research and Development (IR&D) program. During his twenty years with SDC he has led the corporation into a number of advanced technology areas, including programming-language technology, operating-system design, time-sharing, and computer system security. His paper, "Security Control in the ADEPT-50 Time-Sharing System," which was named the outstanding paper at the 1969 AFIPS Fall Joint Computer Conference, is one of the original early contributions to the theory and methodology of computer system security. For three years he managed SDC's Systems Security Department. He directed a large number of security-penetration analyses for nearly all commercial computer systems and a study for the National Bureau of Standards on applications of the NBS data-encryption standard. Earlier, he directed the corporation's ARPA-sponsored research and development activities, which included several studies relating to the design and applications of computer networks. He holds a degree in aeronautical engineering (Massachusetts Institute of Technology, S.B.). He is the author of the 1967 LISP 1.5 Primer, also published in a Japanese edition in 1970. He is listed in Who's Who in the West, and has been active in the ACM, being a past Editor of the OS Department of ACM.

---

The charge given to this session was:

PROGRAM INTEGRITY: What are the audit approaches and techniques for evaluation of program integrity in an ADP environment? Include consideration of operating systems, data base management systems, and application programs.

Program integrity has been defined as that state in which the software is logically complete, and correctly and consistently performs the task for which it was designed and no more. It is within this context that this session should consider the problems associated with evaluation of program integrity.

This session is to identify the audit approaches and techniques currently available or needed that would produce an effective evaluation of (1) the controls exercised by management to ensure program integrity during software development, and (2) the operational reliability and performance assurance of software design and implementation.

---

The consensus report that follows was developed and reviewed by the entire membership of this session.

# Program Integrity Assessment
# A Concensus Report

Clark Weissman

## 1. WHAT IS PROGRAM INTEGRITY?

Coming to grips with program integrity requires definition and assessment of both terms--program and integrity. In the broadest sense, a program is synonymous with a system of programs and includes control software, operating systems, data base management systems, or applications programs. Furthermore, programs are "organic" in that they exist in different forms throughout their life cycle, from requirements, specifications and design, to source and object code.

Integrity concerns, foremost, (1) the correctness with which the program satisfies its requirements, implements its specifications, and does nothing else. But integrity concerns more than correctness. It also relates to (2) satisfying a trained user's expectations of program behavior and to (3) being useful in fulfilling an intended mission. Furthermore, integrity requires that (4) the program can be evaluated to establish a level of trust in it. All four aspects of integrity must hold over the full life cycle of the program.

System integrity is a function of the integrity of the program parts. Usually system integrity is lower than the integrity of its component programs; however, if redundant independent modules are employed to check one another's computation, system integrity can be somewhat higher than the integrity of the component programs.

In summary, program integrity will require management to judge the risks of accepting a level of integrity for the given threat environment. These factors in assessing program integrity in the context of risk are expanded in the balance of this section. The issues presented form a consensus of the session participants.

## 2. A CONTEXT FOR PROGRAM INTEGRITY

Security of a computer system increases with a reduction in (1) system flaws, (2) exposure of system assets, and (3) exploiters. All protection strategies pursue these goals. Program integrity addresses only the first goal--flaw reduction.

However, management can make choices in its protection strategy to trade reductions in integrity for improvement in the other goals to reach a balance for a given threat or budget level. The issues associated with integrity are discussed below.

### 2.1 Programs Change With Time (Life Cycle)

We normally think of programs in their final code or operations stage. Program integrity, however, must be built into programs from the beginning of their development. Programs move through six stages.

1. Organization Mission: The purpose of the system is defined, and responsibilities are divided among the component organizations.

2. Requirements: Mission responsibilities are translated into specific system requirements; i.e., what is to be done. Functions, performance, cost, and other limits are defined.

3. Specifications: Requirements are translated into system specifications for each system element--hardware, software, communications, people, facilities. Specifications define in detail how requirements will be met. Specifications exist at the functional level and at the component level. For the software component, they are called "coding specs." Various schemes exist for documenting coding specs, including flow diagrams, decision tables, table and memory layouts, mathematical algorithms, Parnas-like modules, and most recently, formal specification languages.

4. Code: Specifications are translated into source code in some popular programming language, e.g., PASCAL, PL/1, FORTRAN, COBOL, or machine assembly language, and further translated into run-time object code or micro-code by language compiler or assembly tools.

5. Test and Integration: Before programs are placed into production they are tested individually and as part of the total integrated system. This step is performed in addition to the normal "unit" testing and "debugging" by the programmer of the original code.

6. Operations and Maintenance (O&M): Libraries of source and object code programs are stored for use in the computer facility. From time to time, minor changes are made to these programs by the O&M staff to correct errors, improve performance, expand functions and capabilities, or adapt to new equipment. Control of these changes is part of O&M Configuration Management. O&M can get out of hand, and program integrity can suffer, if major program redesign or modification is attempted at this stage. Major program changes must be viewed as new software that will replace existing modules, and these new modules should be contracted for as were the original programs, beginning at the mission and requirements life-cycle stages.

## 2.2 Visiblity of Relationships Is Lost Between Stages

One of the more significant program integrity problems that results from this staging of software production is the loss, as complexity and detail increase, of visible links between the stages. For example, seldom is it possible to directly relate a module of code back to the mission goal, or system requirement, or even the functional specification. Somehow, the connection gets lost as functions are distributed, level notations are translated to lower-level languages, and programs are made to serve multiple requirements.

This loss of the thread between the initial requirement and the resulting code becomes serious when code must be changed for any purpose. The more significant the modification, the greater is the need for comprehending the interrelations of the parts toward satisfying the mission requirements. Code patching is a major cause of integrity loss, for the "tactical" fix often undermines an unseen "strategic" mission design, leading to even larger problems.

## 2.3 Program Integrity Assessment is Multi-dimensional Problem

Determining when to audit and evaluate in the life-cycle metamorphosis of a program is but one dimension of the integrity assessment problem. Other dimensions include the relevance and severity of the security threat and the methods employed during development to achieve integrity. These dimensions are treated more fully in the following sections.

## 3. RELEVANT THREATS AND THEIR SEVERITY

Threats result from nature and from man. The effects of natural disasters, physical breakdowns, and human error (by builder or user) can be predicted in service interruption or accidental information disclosure. More insidious are the threats from motivated human interlopers. We further divide the human threat into casual and deliberate attacks. The former group deals with individuals who stumble on a flaw or actively browse and seek flaws they can exploit. The latter group is more sophisticated in resources, planning, and methods of attack. These deliberate attack threats are carefully planned by a conspiracy team that creates flaws by modifying running code or planting subversive "trapdoor" functions in the system, application, or library programs. Possibly the worst deliberate threat is from an irrational attack by a disgruntled employee. Since the normal behavior constraints on the attacker -- exposure and capture or expectation of gain -- are absent or distorted, the irrational attack cannot be thwarted by most countermeasures.

Ranking these threats by the severity of the attack and sophistication of the needed countermeasures (high-to-low), produce the following list:

1. IRRATIONAL ATTACK
2. CONSPIRACY TEAM
3. BROWSER
4. STUMBLER
5. HUMAN ERROR
6. NATURAL FAILURE

## 4. METHODS FOR ACHIEVING PROGRAM INTEGRITY

It was established by consensus of the session that program integrity requires the program to be correct, robust, and trustworthy. A correct program provides evidence that it satisfies its mission, requirements, and specifications. By analogy to the auditing of a corporation, the audit of a program's correctness requires evidence equivalent to the corporation's "financial statement."

A robust program includes mechanisms to maintain adequate levels of performance in the face of unexpected behavior in the environment, as will occur from user keystroke or procedural program flaws, operator goofs, etc. The corporate audit analog for these robust mechanisms is the "internal financial control system."

A trustworthy program is one that is well documented, functionally not complex, modular, relatively short in length, integrated into a rigorously structural architecture, and produced as the result of good programming practices and sensible standards. The trustworthiness of programs is the corporate analog of having "generally accepted accounting principles."

### 4.1 Evidence of Correctness

Program validation and verification (V&V) can be either static (done on the source code) or dynamic (done on the running object code).

### 4.1.1 Static Evaluation

Combinations of the following source code examination approaches are currently being used by industry or R&D laboratories:

1. Design Review: This method entails a formal meeting of designers with reviewers (not associated with the deliverable) to scrutinize the product design against mission and requirements. The product design should include narrative documents, logic diagrams, and functional and coding specifications. It may include source code for critical components. Design reviews should be scheduled milestones for each subsystem and major component. Results must be documented and communicated to all participants.

2. Peer Review: The classical scientific method is to invite interested professional peer review and comment on the product at various stages of program life cycle. Design review is one important instance of peer review.

3. Quality Control (QC): A third party (neither customer nor developer) is committed to check the quality of all deliverables during product life cycle. This technique combines 1 and 2 above in a formal, often contractual manner. The QC contractor is selected because of its experience, tools, personnel, and skill in such work.

4. Compiler Checking: Source-code-to-object-code translators (i.e., compilers) have always been used to detect program errors as a QC tool. R&D has suggested new emphasis on this technique as a mechanism for enforcing good programming practice. New languages demand explicit, detailed declarations of a programmer's intent with strong data typing, restricted program scopes, rigid module calling sequences, etc., that force structured programming. The compilers for these languages do extensive and complete checking to enforce the language syntax and semantics, and in some cases generate code for run-time enforcement of program assertions.

5. Automated Analyzers: A number of source-code tools are available that perform some of the syntax and semantic analysis of a compiler, but do not generate object code. Such tools are used to produce flow diagrams, reformat code to aid documentation, produce cross-reference listings and indices for improved library control and use, and to produce test cases for dynamic evaluation. Newer uses are to automatically generate truth assertions about the program to assist in the formal proof of correctness.

6. Formal Proof: Formal proof of program correctness is the leading edge of the state-of-the-art. Basically, the method accepts "correctness criteria" and the "program" as input and produces as output a formal proof (or counter example) that the program satisfies the correctness criteria. In practice, the technique is iterative at each life-cycle stage. At the top level, the correctness criteria are a set of truth assertions and mathematical models of program requirements, and the program is a mathematical specification, both expressed in a "specification language." At the lowest level, the correctness criteria are the prior level's output specifications, and the program is the Higher Order Language (HOL) source code. At each level, these inputs--criteria and program--are processed through a "Verification Condition Generator," which produces a set of conditions to be verified. The "verification conditions," e.g., source program and truth assertions, are processed by a "Theorem Prover" producing a formal mathematical proof of correctness -- i.e., a proof that the source program satisfies the truth assertions. The process can be manual or automated. A number of quite restricted "programs" have been proved both manually and with automated aids, leading to encouraging optimism. However, the problems are great and not fully understood, the progress controversial and slow, and the tools limited and not commercially available.

### 4.1.2 Dynamic Evaluation

Essentially, this approach "runs the program and sees if it works." Unlike static evaluation, dynamic evaluation also tests for errors introduced by the compiler, loader, operating system, libraries and support packages, physical procedures, communication elements, and CPU hardware. Static evaluation tries to exhaust all program conditions; dynamic execution involves real time and is practical only for selected test cases. Therein lies the basic "art" of testing, that is, choosing the best test cases. Many schemes exist. The Department of Defense (DOD) testing requires three stages: (1) unit testing of discrete modules; (2) subsystem testing of the integrated collection of modules; and (3) system testing of the integrated collection of subsystems, actual hardware, and real data. This is a reasonable paradigm for other approaches.

## 4.2 Evidence of Robustness

Unlike correctness, little formal theory exists regarding robustness mechanisms. The best that can be achieved today is to list those methods that have proven effective in existing systems.

### 4.2.1 On-Going Testing

Testing should not end after system delivery and O&M commences. A number of schemes have been successful.

1. Exercising: The system is tested by running simulated operations with known responses that are compared against test results. This is a well known approach in testing DOD systems in the field. A modified version has seen recent application in the commercial sector, where a simulated minicompany is established in a corporation's financial control system so that the auditor can easily observe the system's response to test input to the minicompany. The minicompany approach is also known as the Integrated Test Facility (ITF) method.

2. Flaw Hypothesis Method: In this approach, system flaws are hypothesized based on analogous flaws found in other systems, and are tested for existence on the object system. It is a cost-effective approach to test case selection.

3. Surprise Test: Based on the military Inspector General scheme, the test team arrives unannounced and runs tests on the live system. Such schemes exercise the current live system and uncover possible unauthorized versions or modified operating procedures.

4. Reasonableness Checks: The system is tested on its ability to detect and recover from typical human errors such as typographical errors, out-of-context actions, nonsense commands (e.g., rewind card reader), etc.

5. Error Recovery: The system is tested on its ability to detect and recover from a variety of hardware, communications, power interruptions and surges, and program errors. Of particular interest is restart, check point, and roll-back options.

### 4.2.2 On-Line Monitoring and Control

One class of service found useful in DOD applications involves on-line control by a System Security Officer (SSO). The SSO is concerned with misuse or subversion of the system. To assist in the detection of these and other breaches of system integrity, the SSO has control of built-in surveillance, monitoring, subverter, and journaling software. These programs permit the SSO to test the environment of the system to ensure proper working order, to log current activity, and to investigate individual exception cases. The concepts apply to systems integrity in general, beyond the DOD national security concern. Of particular concern is the management of the system security data base of subject clearances, object classifications, encryption keys, user identifiers (IDs), and passwords.

### 4.2.3 Redundancy

A popular hardware approach to integrity has now found limited application in software. If multiple different algorithms exist for computing a result, these can be computed redundantly by different, independent modules, as part of the operational software, and the results can be compared and exceptions reported (possibly to the SSO).

### 4.2.4 Support Control

Confidence in the system's robust behavior can be attributed to the facility management and O&M procedures. These fall into three areas:

1. Code Control: Good program libraries are required to permit selective access to system and user code, and to permit rational change procedures for error correction and software upgrades.
2. Error Control: Errors will occur and will need to be reported, and appropriate actions will need to be taken.
3. Documentation Control: Source program libraries are one form of documents. User and system manuals, and other forms of English documentation must be kept current to the level of the software in use if errors are not to be introduced by dated descriptions and procedures.

## 4.3 Evidence of Trustworthiness

Trusted software is obtained from a successful blend of factors: (1) experienced personnel, (2) organized software development, and (3) good tools. Each of these factors may be developed in a variety of ways.

### 4.3.1 People

Skilled people can be as much as twenty times more effective than less skilled people in the quality of code they produce. Trustworthiness of code is improved by demonstrating good personnel selection and training practices, and by personnel experience. The DOD employs a system of background investigations to screen personnel for suitability to various levels of job sensitivity.

### 4.3.2 Software Development

One trusts better-made programs. Since a software product mirrors its production management, better production methods yield better products. This suggests a trustworthiness evaluation method, i.e., scrutiny of development practices yields insight into product trustworthiness. The following steps can be taken to perform a comprehensive review of the programming practices employed:

1. Assess the standards, quality control methods, and management controls employed. Are they well documented, read, and used?
2. Explore methods used to make production status visible to management. Are the data meaningful?
3. Determine the degree of automation employed to enforce stated management and programming practices.
4. Use an audit team to examine the programs in depth for compliance with stated management and programming practices. Are they well documented?
5. Examine procedures and history of corrective action to problems detected in prior audits, reviews, and tests. Was meaningful action taken to rectify problems and did production improve?

### 4.3.3 Tools

Good tools amplify skills and can aid all aspects of trust evaluation by giving confidence in the quality, timeliness, and control of program development. Among the tools of significance, are:

1. Production Tools: Language preprocessors and compilers, test case generators, program production libraries, proof verifiers, theorem provers, assertion generators.

2. Management Tools: Configuration controls, status monitors, standards, quality control procedures, error and change controls, cost controls, module-to-mission linkage threads.

3. Documentation Tools: Flow charters, word processors, document libraries, and change controls.

4. Audit Tools: Flaw lists, penetrations analyses, test cases, flow charters, and redundant but independent production tools to test repeatability (e.g., compile a randomly selected module with the audit compiler and test the object code produced by substituting it in the system).

## 5.0 PROGRAM INTEGRITY IMPACTS OTHER SESSIONS

Our broad interpretation of program integrity as a multi-dimensional problem impacts the discussions of other workshop sessions. We summarize these considerations for each session below.

### 5.1 Internal Audit Standards

It is imperative that internal audit standards reflect the guidance presented in this session. Of particular concern is our recommendation for agencies to perform self assessment (cf. 6.3 Recommendations).

### 5.2 Qualifications and Training

Since program integrity is a complex technical subject, auditors need to draw upon independent, experienced, competent, professional, and technical computer science talent.

## 5.3 Security Administration

One area often overlooked is the management of system control data, upon which program integrity is dependent. This must fall to security administration, possibly in the form of a System Security Officer, (SSO). Data included in this is described in paragraph 4.2.2, On-Line Monitoring and Control. Furthermore, much of our discussion in Section 4.2, Evidence of Robustness, is pertinent to security administration.

## 5.4 Audit Considerations In Various System Environments

We feel that program integrity comments herein apply to all software, regardless of application, including distributed systems, communications processors and smart terminals, controllers, and microcode.

## 5.5 Administrative and Physical Controls

The whole facility management mechanism for controlling access and changes to software stored off-line is a cornerstone of trusted software. Furthermore, the issues of the on-line System Security Officer and remedial actions for backup and recovery impact physical controls. We also point out that system integrity can often be maintained at an acceptable risk level even with flawed programs, by increasing physical access controls to reduce the exploiter population. This does not preclude natural failure and human error.

## 5.6 Program Integrity

Not applicable.

## 5.7 Data Integrity

By definition, data integrity does not impact program integrity since system control data is considered part of program integrity. On the other hand, data integrity cannot exist without program integrity. Where existing software of dubious integrity is employed, caution is in order, and steps should be taken to reduce the risks (cf. 6.1 Recommendations).

### 5.8 Communications

See paragraph 5.4 above

### 5.9 Post-Processing Audit Tools and Techniques

All of Section 4, Methods for Achieving Program Integrity, is relevant.

### 5.10 Interactive Audit Tools and Techniques

All of Section 4, Methods for Achieving Program Integrity, is relevant.

## 6.0 RECOMMENDATIONS

The following consensus recommendations are made regarding the audit and evaluation of program integrity:

### 6.1 Existing Software

- Be cautious in assuming program integrity, especially with sensitive applications.

- Although limited, tools and techniques for auditing and evaluating program integrity do exist. They should be applied via a careful risk management analysis.

- o Reduce the effect of the lack of program integrity by improving physical, procedural, and management control, and upgrade the O&M organization.

- o Reduce the exploiter population by access controls and user authorization screening.

- o Reduce the asset exposure by removing the asset from the system when it is not in use. Encryption may be used to accomplish the same effect.

## 6.2 Future Software

- o Improve the production process with rigorous enforcement of good programming practices throughout the program's full life cycle.

- o Assure program integrity compliance at each development stage from mission objectives, functional requirements, system specification, HOL code, and O&M.

## 6.3 Organization Actions

- o Each organization must do a self-assessment of its threats and involvement in the life cycle of the programs it uses. The earlier the involvement, the better, depending on the degree of concern for security threats.

- o Organizations should prepare detailed guidelines for development or acquisition of existing and future software, with consideration given to the auditability of program integrity.

# 7. BIBLIOGRAPHY

Abbott, R.P. et al., "Security Analysis and Enhancements of Computer Operating Systems,"
NBS, NBSIR 76-1041, April 1976.

Branstad, D.K., "Privacy and Protection in Operating Systems,"
IEEE Computer, Jan. 1973, pp 43-46.

Bushkin, A.A., S. I. Scheen, "The Privacy Act of 1974: A Reference Manual for Compliance,"
SDC, May 1976, 183p, $15.00.

Committee on Govt. Operations, U.S. Senate, "Problems Associated with Computer Technology in Federal Programs and Private Industry,"
U.S. Govt. Printing Office, June 1976, 448 p, $3.95.

Committee on Govt. Operations, U.S. Senate, "Computer Security in Federal Programs,"
U.S. Govt. Printing Office, Feb. 1977, 298 p, $2.80.

Engelman, C., "Audit and Surveillance of Multi-Level Computing Systems,"
MITRE Corp., MTR-3207, June, 1975.

Fagan, M.E., "Design and Code Inspections to Reduce Errors in Program Development,"
IBM Systems Journal, Vol 15, No. 3 1976, PP 152-211.

Goodenough, J.B., "Exception Handling: Issues and a Proposed Notation,"
CACM 18, 12, Dec. 1975, pp 683-696.

Gwinn, C.J., "A Concept of Operations for the WWMCCS ADP Security Officer (WASO),"
SDC, TM-WD-7828, Jan. 1977.

Hecht, H., "Fault-Tolerant Software for Real-Time Applications,"
Computing Surveys, 8, 4, Dec. 1976.

Hollingworth, D., S. Glaseman, M. Hopwood, "Security Test and Evaluation Tools: An Approach to Operating System Security Analysis,"
The Rand Corporation, P-5298, Sept. 1974.

Linde, R.R., "Operating System Penetration,"
AFIPS Conf. Proc., Vol. 44, 1975, pp 361-368.

Linden, T.A., "A Summary of Progress Toward Proving Program Correctness,"
AFIPS Conf. Proc. FJCC, Vol. 41, Part 1, 1972, pp 201-211.

Linden, T.A. "Operating System Structures to Support Security and Reliable Software,"
Computing Surveys, 8, 4, Dec. 1976.

Mair, W.C., D. R. Wood, and K. W. Davis,
Computer Control & Audit, The Institute of Internal Auditors, 2nd Edition, 1976.

Nielson, N.R., et al., "Computer System Integrity Safeguards - System Integrity Maintenance,"
NSF-SRI Project 4059, Grant # DCR 74-23774, Oct. 1976.

Ruder, B. and J.D.MADDEN, "Development of Technical Specifications to Serve as a Basis for Federal Guidelines to Prevent Intentional Computer Misuse,"
NBS-SRI Project 5798, Jan. 1977.

Webb, D., W. Frickel (Ed.), "Proceedings of the NSF Software Auditing Workshop,"
NSF-LLL Conf-760116, Jan. 1976.

Weissman, C., "System Security Analysis/Certification Methodology and Results,"
SDC SP-3728, Oct. 1973.

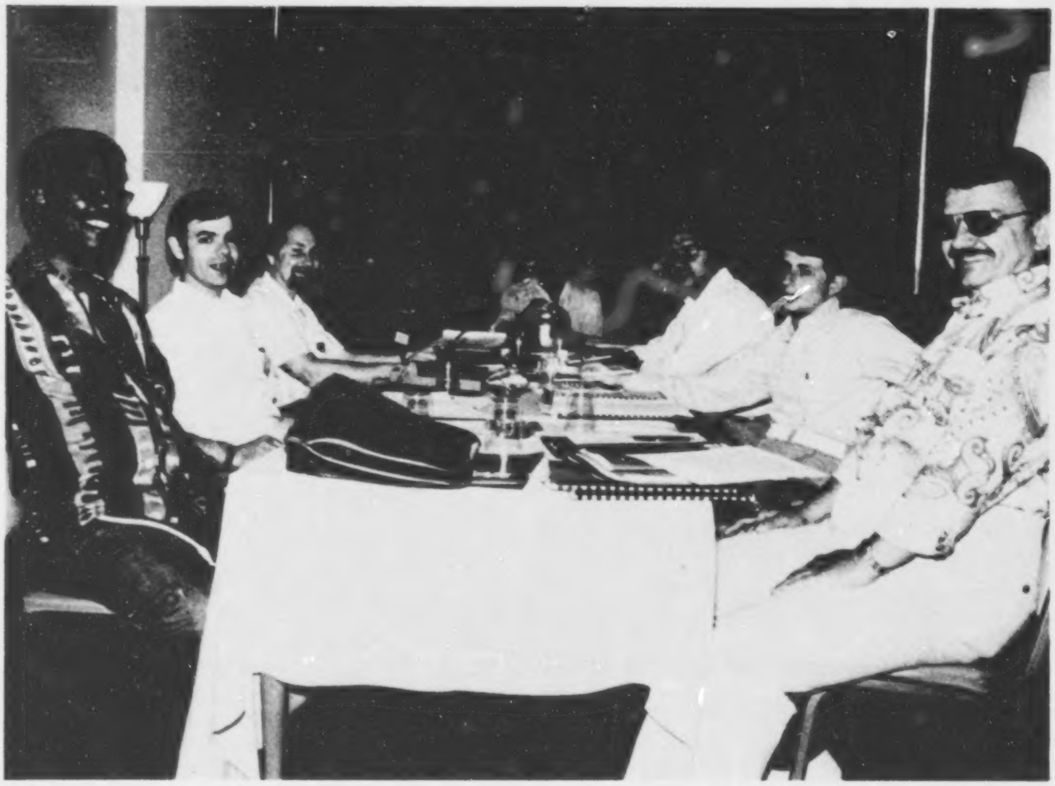
# PART IX: DATA INTEGRITY

Chairperson: Leonard I. Krauss
Ernst & Ernst

Participants:

Robert P. Abbott
EDP Audit Controls
N. D. Babic
Atlantic Richfield Company
Dwight Catherwood
Ernst & Ernst
Stuart W. Katzke, Recorder
National Bureau of Standards

Aileen MacGahan
Chase Manhattan Bank
Hubert S. Obstgarten
Ernst & Ernst
Barry S. Silverman
Gulf & Western Industries, Inc.



From left to right: Robert P. Abbott, John Panagacos (visiting session coordinator), Stuart W. Katzke, Barry S. Silverman, Leonard I. Krauss, Aileen MacGahan, Dwight Catherwood, Hubert S. Obstgarten, N. D. Babic

---

Note: Titles and addresses of attendees can be found in Appendix A.

# EDITORS' NOTE

A brief biography of the Session Chairperson follows:

Mr. Leonard I. Krauss is a Manager, Management Consulting Services, in the New York office of Ernst & Ernst where he is a consultant to management in the areas of planning and control systems, data processing management, and information system security. His system planning and development experience includes a variety of computer applications for financial institutions, manufacturers, service companies, and other organizations. Mr. Krauss was previously associated with IBM and Union Carbide. He has also been an officer and director of several companies and held positions as Director of Management Systems and Project Manager for Advanced Management Systems. A registered professional industrial engineer, he has earned the CDP (Certification in Data Processing) and is the author of three popular books: Computer-Based Management Information Systems, Administering and Controlling the Company Data Processing Function, and SAFE: Security Audit and Field Evaluation for Computer Facilities and Information Systems. He holds a MBA in Business Management Systems from Fairleigh Dickinson University and a BS in Industrial Engineering from Pennsylvania State University. Mr. Krauss is a frequent speaker at international management conferences.

---

The charge given to this session was:

> DATA INTEGRITY: What are the audit approaches and techniques for evaluation of data integrity in an ADP environment?

Data integrity is the state that exists when computerized data is the same as that in the source documentation and has not been exposed to accidental alteration or destruction. It includes both data accuracy and data protection. Computer generated data involved in automatic decision making process should also be considered.

Data integrity is an area that has traditionally been addressed by the audit community. This session is to identify those audit approaches and techniques that are unique to an ADP environment and have not been subjected to extensive coverage in the literature.

---

The consensus report that follows was reviewed by the entire membership of this group. It was written by L. I. Krauss and S. W. Katzke.

# Data Integrity Auditing:
# A Framework for Standards Development

## 1. INTRODUCTION

An audit and evaluation of ADP security calls for an examination of the system of safeguards used to prevent, deter, detect, and limit the impact of undesirable events.

An adequate system of safeguards is one having design, implementation, and compliance characteristics appropriate to the magnitude of the risks and exposures assoicated with undesirable events. Examples of undesirable events include: an ADP center file, an unauthorized update to data base records, and an illegal tap on a data communications line. Examples of exposures include: destruction of assets, erroneous disbursement of funds, embezzlement and fraud, disclosure of personal or proprietary information, political/military/competitive disadvantage, faulty decisions, extra operating expense, legal and contractual penalties, interruption of critical ADP services, and loss of life.

In auditing and evaluating the system of safeguards for ADP, there will be factors that have either a direct or an indirect bearing on data integrity. The audit and evaluation of data integrity safeguards, for purposes of this report, is limited to factors having a direct bearing and which pertain to a particular ADP application selected for examination (data ingegrity audits are conducted on an application-by-application basis).

Factors that have an indirect bearing, for purposes of this report, include physical, operational, administrative, and software security measures which are part of the more general system of safeguards and which are not usually peculiar to any one ADP application. These general security measures are recognized as being vitally important--so much so that it may be virtually impossible to have adequate data integrity safeguards for an ADP application in an environment where there are significant inadequacies in the system of general safeguards.

Inadequacies in the system of data integrity safeguards are sometimes indicative of weaknesses in the general security system, in much the same way that abnormalities in a person's blood pressure and cell counts indicate a malfunction in some other part of the body. The auditor must be alert to such possibilities and point them out, even though the scope of the data integrity examination does not encompass a detailed study of them.

Specifically, a data integrity audit must evaluate the policies and procedures that directly affect the quality of all forms of data (e.g., source, entry, processed, and output) in the application system under review. As a prerequisite to a data integrity audit, the auditor must have a clear understanding of the definition of data integrity and the objective and scope of the audit. To perform the audit, the auditor must first formulate an approach or work plan and then use appropriate and acceptable methods for conducting the audit. During the course of the audit, it is necessary that the definition of data integrity and the objective of the audit always be kept in mind.

Section 2 provides a definition of data integrity. Subsequent sections discuss the objectives, scope, approach and methods for conducting the data integrity audit.

## 2. DEFINITION OF DATA INTEGRITY

Data integrity is the state that exists when data are (within defined limits of reliability) accurate, consistent, authorized, valid, complete, unambiguous, and processed according to specifications in a timely manner. It is important that this definition be constantly referred to during the course of a data integrity audit.

## 3. OBJECTIVE OF THE DATA INTEGRITY AUDIT

Keeping the definition of data integrity in mind, the objective of a data integrity audit of a particular application system is to render an objective opinion based on an evaluation by qualified individual(s) as to the:

(1) Compliance with existing policies and procedures for maintaining data integrity

(2) Adequacy of the existing policies and procedures

In addition, as a result of the compliance and adequacy evaluations, corrective actions may be recommended to enhance the data integrity of the application system. Furthermore, it is essential that the date the audit is completed be recorded since it represents a specific reference point. Any assumptions about the state of the system's data integrity made after this date become less and less valid as time goes on.

When conducting the data integrity audit, it is important that the objective of the audit be kept in mind.

## 4. SCOPE OF THE DATA INTEGRITY AUDIT

The scope of the data integrity audit is necessarily broad since data associated with an application system exist in many forms and are affected by policies and procedures in different parts of the system and in the organization which provides and uses the data. However, it is not generally practical to have a data integrity audit include examinations of all related system areas that affect data integrity. Among the functions that should be included as part of other audit procedures would be verifications of:

- Underlying physical facts represented by data elements (e.g., counts, confirmation, observations)
- Software integrity and software maintenance controls
- Physical, administrative, and operational security

To achieve the previously stated objective of a data integrity audit, the following areas should be evaluated with respect to compliance and adequacy of existing policies and procedures and appropriate recommendations should be made when they will improve data integrity.

Reliability of the Data Source. The sources of data for an automated application system will vary according to the application. They may range from data collected manually to data collected by automated data capture devices such as automatic teller machines and point-of-sale terminals. In some cases, source data may be transmitted to the application system by feeder systems.

Whatever the collection method, it must be shown that the sources are reliable ones. This requires the auditor to verify that a particular source of data is the designated and authorized one, that the data obtained is current and timely, that the data is captured as close to the source as practical, and that adequate separation of duties exists between the creation/collection and the authorization of source data.

Source Data Preparation. Once captured, raw source data must, in most cases, be prepared for entry into the ADP system. Data preparation requires the conversion of raw data, in some instances using a codification scheme, and transcription of the converted data on to additional source documents. Following conversion and transcription, the data may be further converted to a machine-readable form (e.g., keypunching) prior to entry into the ADP system. In situations where the source data is collected in automated form or is keyed in directly to an on-line system, the data preparation function may be minimal. Data preparation is highly susceptible to human errors. Furthermore, it is a likely place for the insertion and manipulation of records for fraudulent purposes.

To evaluate source data preparation controls, it is necessary to review the data preparation policies as well as the data preparation procedures and training programs. The existance of appropriate control records for determining accuracy, authorization, and completeness of source data records should be verified. Additionally, data codification structures should be reviewed to assure consistency between data originating from different sources or source documents and to assure accuracy during conversion.

Data Entry Control. Methods for entering data into the ADP system will vary widely from application to application. In some systems data capture and entry take place simultaneously through devices such as automatic teller machines, point-of-sale equipment, and optical character readers. In others, keying of data may take place on-line, or in key-to-tape and key-to-disk devices. In some cases, data may enter the application system through other systems. Like data preparation, data entry is highly error-prone. It is also a likely place for the insertion and manipulation of records for fraudulent purposes. Whenever possible, detection and correction procedures should be used to prevent erroneous data from entering and corrupting the ADP system.

To evaluate the data entry control procedures, the auditor should first review the procedures being utilized, including criteria for accuracy, completeness, and authorization. Training programs and plans should be reviewed as well as instructions for data entry that are given to data entry personnel. It is mandatory to review the error detection and correction procedures and to determine if they are adhered to.

Data Input Acceptance Control. Input data (transactions, master file and data base maintenance, tables, etc.) can pass through several organizational areas as source data is captured, prepared, and entered into the ADP system. In some cases, data enters the ADP system through feeder systems from distributed computational points of the organization or from outside sources. When the custody of input data changes hands, up to and including the point where it is entered into the application system, there should be data input acceptance control procedures which define accountability for access, authentication, and accuracy of the input data.

As part of a data integrity audit, it is essential that input data acceptance control procedures be evaluated at each control point where the input data changes hands. This evaluation should include a review of input data acceptance control prodecures for the purpose of accountability and a review of input data access and authentication controls. In addition, the existance of appropriate control records for determining the accuracy and completeness of input data records should be verified.

Data Validation and Error Correction. Prior to the use of input data in an ADP system, the data should be carefully validated (i.e., edited, checked) to detect erroneous data. If errors are found, they should be corrected and reentered into the system. Thus, when conducting a data integrity audit, it is necessary to evaluate the data validation and error correction procedures. This includes a thorough review of existing procedures--including recommendations for corrective action when necessary. In cases where manual procedures for data validation have been replaced by automated controls, the automated controls should be reviewed to assure they perform the intended validation functions. Finally, controls for handling error rejects, corrections and data reentry should be reviewed.

Processing Specifications. A key factor affecting the data integrity of an application system is the assurance that data is processed in accordance with specified formulas or rules. Ideally, these processing specifications should be formalized and recorded with the system documentation. Often these specifications are informal, not recorded in any form of documentation, and are known only by a few individuals. In some cases, the processing specifications may exist in a combination of states.

Whatever the form of the processing specifications, they must be evaluated as part of the data integrity audit. This evaluation should include the review of all processing specifications and the review of processing controls both within the ADP system and between the system components that can affect the processing. It would cover controls, procedures, and safeguards such as those pertaining to processing of proper files, internally generated data, program sequence, privacy transformations, and access (user identification/authentication/authorization). In addition, backup, recovery, and restart procedures should be reviewed as part of an evaluation of the processing specification of an application system.

Keep in mind that a secure data system operates without surprises, meaning that it behaves as intended and according to specifications, fails according to specifications, and gives a predictable response when it is functioning as expected as well as when it is failing.

Output Controls and Distribution Procedures. The accuracy, reliability and timeliness of computerized output and the access to and distribution of the output to authorized individuals are factors affecting data integrity. As part of a data integrity audit, the internal (i.e., automated) controls that ensure the quality of output reports and generated magnetic media should be evaluated, as should the access and distribution procedures for the output. In addition, output forms control procedures should be reviewed.

Auditability. The ability to meet the objectives of a data integrity audit depends, to a large degree, on the auditability of the application system under review. Auditability requires that procedures and policies are in place to assure that the information and documentation necessary to perform the data integrity audit is available, timely and adequate. Thus, as part of a data integrity audit, the auditability of the ADP system should be evaluated.

This evaluation should include a review of the quality and quantity of data retained for auditing, backup, and recovery purposes, a review of the length of time that such is retained, and a review of the currency and completeness of the system documentation. In addition, an audit trail mechanism should exist and its documentation should be current and complete. In general, an evaluation of auditability should include a review of policies and procedures for maintaining information that supports audit objectives.

## 5. APPROACH TO A DATA INTEGRITY AUDIT

The success of a data integrity audit depends upon the thorough formulation of an approach or work plan for auditing the application system. During the development of the work plan, it is important to keep in focus the definition of data integrity, and the objective and scope of a data integrity audit. With these in mind, the formulation of a work plan should include the following steps:

- Obtain an understanding of the organizations, policies, procedures and practices pertaining to the application system under review.
- Obtain a general understanding of the application system, including factors such as the intended purpose or function, the requirements of the user community, the source and flow of input data, the processing requirements, the output requirements and relevant time constraints.
- Identify specific data files. inputs, processing steps, interfaces with other applications and outputs which are utilized throughout the application.
- Identify specific control features or points that affect data integrity.
- Identify potential threats to data integrity for emphasis when reviewing the application.
- Decide upon the methodology (i.e., audit tools and methods) that will be used when conducting the audit.
- Obtain an understanding of the human factors that affect the application system, including the human engineering aspects of the user interface as well as personnel areas such as hiring and termination practices, employee moral, vacation and job rotation.
- Obtain an understanding of the hardware, software and systems technologies used in the application system.
- Obtain an understanding of the training and continuing education programs offered by the organization.
- Obtain an understanding of the application system's development, implementation and maintenance controls.
- Decide on the form of reporting the findings, conclusions, and recommendations of the audit.

- Decide on review procedures for the audit that will assure high technical quality of the audit.
- Decide on audit staffing and project control methods.

Once the objective, scope, approach and work plan for a data integrity audit of a particular application system have been established, the audit should be conducted using appropriate audit tools and methods. Following the audit, a draft report of findings, conclusions, and recommendations should be prepared by the auditors, reviewed with appropriate management personnel, and submitted in final form. If corrective measures have been recommended, the managers ultimately responsible for data integrity should be required to respond, in writing, regarding planned actions.

## 6. METHODS FOR DATA INTEGRITY AUDITING

In conducting the audit, a variety of audit tools and methods* may be used to determine the compliance with and adequacy of the policies and procedures intended to insure data integrity in the application system under review. Examples are discussed below:

- Confirmation with users, customers, vendors or others familiar enough with the data to assure its accuracy, completeness, and consistency. (Except as a spot-checking technique, confirmation would be part of other auditing procedures. However, the results of a data integrity audit should be carefully considered in deciding the objectives and scope of auditing through confirmation.)
- Sampling techniques where portions of the data population, usually randomly selected items, are inspected to determine the state of the data. Discovery sampling is intended to uncover the existence of errors. If errors are found, additional samples may be taken and estimation sampling applied to them. Estimation sampling is used to determine the extent of erronous data in a data base by applying statistical techniques to a sample of the data for the purpose of predicting the amount of contamination. Attribute sampling may be used to select records based on inconsistencies in characteristics within the record itself (for example, an accounts receivable balance that exceeds the credit limit by 10 percent or more). It may also be used to test a population for the presence of particular characteristics.

---

*Over 25 audit techniques are discussed in Audit Practices report, published in 1977 by The Institute of Internal Auditors (Altamonte Springs, Florida 32701). This was one of the reports resulting from the SAC (Systems Auditability and Control) Study.

- Parallel processing checks for correct processing of data by the application system. With this technique, data processed by the application system would be processed by an independent program performing the same functions. The two results would then be compared.

- Integrated Test Facility (ITF) allows the auditor to continuously monitor the performance of the application system by incorporating dummy master records into the data base. Once these records are in place, the auditor can process test transactions against them by including the test transactions with the live data during the normal processing cycle. The auditor can then compare the processing results with predetermined results.

- System Control Audit Review Files (SCARF) involves the placement of auditor-designed tests within the application system program code. During normal processing, the audit tests are performed on the processed data. Either processing exception or predetermined sample solution criteria is used to extract the desired records and write them on a review file. The auditor can then examine the review file and draw appropriate conclusions.

- Tracing gives the auditor the ability to follow (trace) specifically marked or tagged input transactions as they are being processed by the application system. It requires the insertion of additional code into the application system and an extra field in the transactions for the tag. This code generates a processing record or trail for the marked transactions which can be analyzed by the auditor to determine if the processing is correct.

- Observation of personnel by visual, electronic or photographic means can assist the auditor in determining compliance with and adequacy of existing policies and procedures and in determining erroneous or fraudulent behavior.

- Analysis by interrogation of existing data consists of examining accounts, balances or other indicative and history data to determine if incompatible relational conditions exist (e.g., mismatches between the data and source documents or other records).

- Test decks or test data can be used for the testing of new or modified applications programs before they are placed in production or for testing the application system's processing integrity. In either case, a set of test input transactions is processed by the application system and the results are compared with predetermined results.

- Interviews with management, users and systems personnel on either a formal or informal basis can be used to supplement system documentation, provide a better understanding of existing policies and procedures, and to verify compliance with these policies and procedures.

- Program source code review, for the purpose of a data integrity audit, should be used only as a last resort. When information about file formats, processing steps and control descriptions is needed, it is better to use other documented sources such as record layouts, system flow charts, program logic flow charts, and program descriptions. Analysis of program listings is very time consuming and generally requires skill in programming and detailed knowledge of the specific programming language. In cases where other documentation is inadequate or nonexistent, program listings usually provide the most up-to-date information. Consequently, limited review of source code may be necessary.

- Questionnnaires are a traditional audit tool for obtaining information about an application system and for evaluating controls to determine adequacy and compliance. They are most effective when tailored for particular types of applications such as payroll, purchasing, inventory, etc. and provide preliminary information for a more thorough evaluation.

- Code analysis and mapping is accomplished by a software measurement tool that analyzes a program during its execution to determine how many times each program statement was executed. While its original purpose was to aid program development, mapping can be used by auditors to evaluate program operation. However, its use requires that the auditor have a basic level of understanding of both the application system's structure and application programming.

- Automatic flowcharting software consists of software routines which convert program source statements into flow charts which graphically describe the program logic. The use of flowcharting software makes it easier to understand the logic of a program and also guarantees that the auditor has a current flow chart when he is reviewing the application system. However, reading the flow charts usually requires some programming expertise. Flow charts are most useful when the auditor is looking at particular problem areas. As with source code review, reading logic flowcharts may be of limited value in auditing for data integrity.

- Procedural walk-throughs consist of the auditor following the flow of specific transactions through all states of the system--from their source until their processing is completed. An auditor can perform a walk-through to verify his understanding of how the system works, to check that the system functions as the existing documentation describes and, in cases where there is inadequate or no documentation, to determine actual system operation. This method, when used in conjunction with code analysis and mapping and automatic flowcharting software, can provide the auditor with an overall understanding of both the manual and automated functions in the system.

- Undercover observations give the auditor a chance to view normal system operations without the system personnel being aware that they are being observed. This allows the auditor to determine if stated policies and procedures are being complied with on a day-to-day basis and to detect actions that might not be performed if the system's personnel knew they were being observed. Such actions might include employee fraud or embezzlement.

- Surprise visits, like undercover observations, allow the auditor to view the system under normal operating conditions. Advanced notice of an audit tends to increase anxiety and induce abnormally good behavior in personnel.

- Analysis of system activity logs, such as transaction, access, library, operator and console logs, will aid the auditor in evaluating compliance with existing policies and procedures. Following the analysis of the logs, the auditor may decide that the logs are not adequate for their intended purpose or, based upon the analysis, that existing policies and procedures are not adequate or not being complied with.

- Continuous monitoring and surveillance software. Software monitors are programs which execute concurrently with the application system in an attempt to determine resource usage and system bottlenecks. Surveillance software provides real-time monitoring of the application system in an attempt to detect erroneous or exceptional events during processing. Specific examples of surveillance software are the Integrated Test Facility and the System Control Audit Review Files discussed previously.

# PART X: COMMUNICATIONS

Chairperson: Jerry FitzGerald
Stanford Research Institute

Participants:

Dennis K. Branstad, Recorder
National Bureau of Standards
Lynne E. Devnew
IBM Corporation
Milton Lieberman
Merrill, Lynch, Pierce, Fenner, and Smith
Robert Morris
American Telephone and Telegraph
Fred A. Stahl
Columbia University
Ken Sussman
Bell Laboratories

From left to right: Ken Sussman, Lynne E. Devnew, Jerry FitzGerald, Robert Morris, Milton Lieberman, Fred A. Stahl, Dennis K. Branstad.

---

Note: Titles and addresses of attendees can be found in Appendix A

## EDITORS' NOTE

A brief biography of the Session Chairperson follows:

Dr. Jerry FitzGerald was formerly a Senior Management Systems Consultant at the Stanford Research Institute and is currently President of Jerry FitzGerald & Associates. He has also been a state university Associate Professor in business data processing and EDP auditing, a systems engineer in a major medical center, a senior systems analyst with a computer manufacturer, and an industrial engineer with a pharmaceutical firm. His specialized professional competence lies in: planning/development of both computer-based and manually oriented systems for financial/industrial organizations, hospitals/medical centers, and educational institutions. His expertise includes EDP auditing, EDP security, and data communications. His degrees are in Industrial Engineering (Michigan State U., BS) Business Administration (U. of Santa Clara, MBA), and, from Claremont Graduate School, an MA in Economics and a Ph.D. in Business. His most recent publications include: Fundamentals of Data Communications, Wiley/Hamilton (in press), "In-House Staff Versus Outside Consultants", Proc. of the Academy of Management, 35th Ann. Mtg., New Orleans, La., 1975; "Auditing EDP Systems; Eight Areas of Control", Data: Its Use, Organization, and Management, Proc. of Pacific '75 ACM Conf.; and a textbook, Fundamentals of Systems Analysis, John Wiley and Sons, 1973. He is a member of the Academy of Management.

The charge given to this session was:

> COMMUNICATIONS: What are the audit approaches and techniques for evaluation of communications in an ADP environment? Include considerations of hardware, software, and protocols.

Data communications can be simply defined as the interchange of data messages from one point to another over communications channels. Dedicated or dial-up facilities can be employed in a variety of network configurations.

This session is to analyze the various communication environments and identify the major aspects that the auditor must consider to conduct an effective evaluation. Audit approaches and techniques for such an evaluation should be developed.

The consensus report that follows was developed and reviewed by the entire membership of this session.

# AUDIT AND CONTROL OF
# DATA COMMUNICATIONS NETWORKS
## A Consensus Report

Jerry FitzGerald, Chairman
and (alphabetically listed)
Dennis K. Branstad, Lynne E. Devnew, Milton Lieberman,
Robert Morris, Fred A. Stahl, Ken Sussman

## 1. INTRODUCTION

This paper presents guidelines, rather than a set of standards, that can be utilized when conducting a data communication security audit. It is the intent of the committee that this paper form a basis from which EDP auditors, either in government or private industry, can develop methodologies to audit their organizations' data communication network. Further research in this area might enlarge upon these guidelines to develop a set of standards that could be utilized for auditing government or private-industry data communication networks.

### Definition of the Special Data Communication Audit

There are many types of audits that can be performed. This paper addresses a special type of audit that involves only those computerized systems that utilize a data communication network and further is limited to the review of the data communications portion of these systems. A special data communications audit involves the end-to-end network, and all of its associated hardware, software, and people. An audit of this nature should be conducted periodically to determine whether the information being transmitted over the network is being properly safeguarded from its point of origination to its final destination. The frequency of the audit should be based on the sensitivity of the data and applications utilizing the network. Additionally, a data communications audit should be conducted whenever there is a reasonable doubt as to the overall integrity of the network.

### The Exposures

Data communications networks can be subjected to several categories of exposure including those to which any other business information system might be subjected. For the purposes of this audit the participants in this workshop identified the exposures to be (these are defined in Section 3. of this paper):

- Errors and omissions
- Disaster and disruptions
- Loss of integrity
- Disclosure
- Defalcation
- Theft of resources.

## How to Audit a Data Communications Network

It is assumed that the EDP auditor conducting a data communications audit has a general understanding of how data communication systems operate, i.e., how messages are transmitted over communication links.

It is the opinion of the committee that a data communication audit should be conducted as a transaction flow analysis. Transaction flow analysis is a technique of tracing a transaction or group of transactions from the point of original entry (the terminal), through the data communication network, to the computer. Using this technique, the auditor is able to evaluate the flow of transactions, the hardware/software, the transmission media, and, in some cases, the manual interface controls that involve the people who run the network. The committee believes that it is wise for the auditor to trace the flow of transactions starting at both ends of the network (terminal and computer) and to reconcile the findings. The audit should be conducted for the general data communications system, as well as for each sensitive application using the data communications network.

To assist with the audit, this paper depicts a matrix that matches the various resources (terminals, distributed intelligence, communication lines, and the like) with the previously mentioned exposures (errors and omissions, disaster/disruptions, loss of integrity, and the like) so the auditor can determine which resource may be subject to what type of exposure. The resources are listed below and are defined in Section 3 of this paper (Figure 1 depicts the resources from terminals to computer):

- Terminals
- Distributed intelligence
- Modems
- Local loop
- Lines: dial-up, point-to-point, multipoint, and loop
- Multiplexor, concentrator, switch
- Front end
- Computer

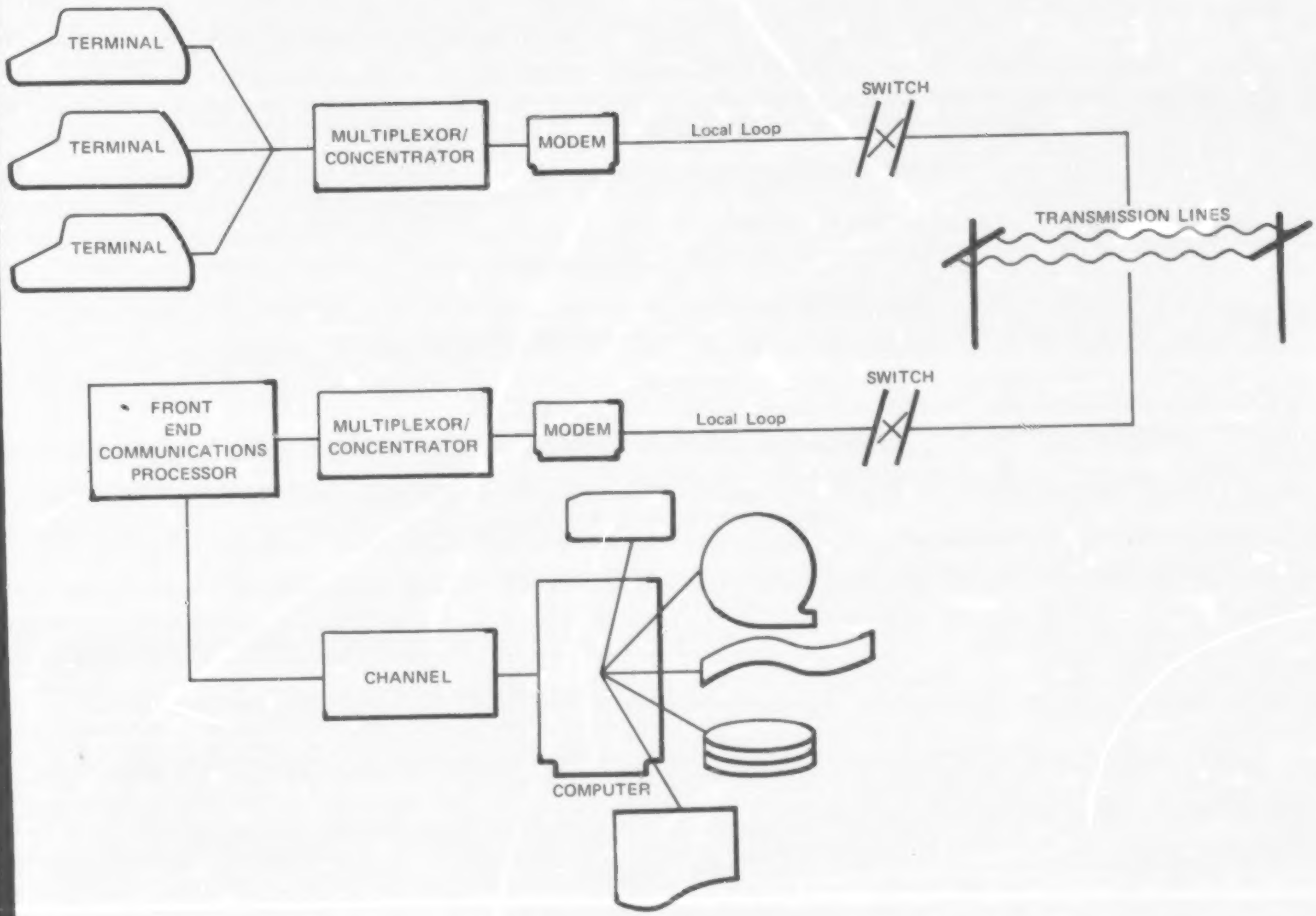


FIGURE I END TO END DATA COMMUNICATION NETWORK

- Software
- People.

The safeguard matrix (Table 1) lists resources down the left-hand vertical axis, and the exposures across the top horizontal axis. Within each of the cells of the matrix, various safeguards are listed that the auditor should consider when reviewing the security of the network. The safeguards are listed below and are defined in Section 3 of this paper:

(1) Physical security controls

(2) Audit trails

(3) Back-up

(4) Recovery procedures

(5) Error detection/correction

(6) Authentication

(7) Encryption

(8) Operational procedures

(9) Preventive maintenance

(10) Format checking

(11) Insurance

(12) Legal contract

(13) Fault isolation/diagnostics

(14) Training/education

(15) Documentation

(16) Testing

(17) Reporting and statistics.

In conducting an audit, any resource that is subject to an exposure should have some type of safeguard that the auditor must consider. In doing this, the auditor would "walk through" the data communications network and evaluate the safeguards listed for each specific resource versus its exposure with regard to the specific application system. This is an important point; the auditor should use the matrix to review the communication security in light of each of the specific applications that are utilizing the data communications network.

## Limitations

This paper is intended to be a basis for further research that may lead to industry/government standards for conducting data communication audits. The matrix of resources versus exposures should be utilized to

Table 1

MATRIX OF SAFEGUARDS TO AUDIT A DATA COMMUNICATIONS NETWORK

| | Exposures | | | | | |
|---|---|---|---|---|---|---|
| Resources | Errors & omissions | Disasters & disruptions | Loss of integrity | Disclosure | Defalcation | Theft of resources |
| Terminals | 2,3,5, 9,13 | 1,3,4, 8,11 | 1,2,5, 6,8,13 | 1,2,6, 11,13, 17 | 1,2,6, 8 | 1,2,6, 17 |
| Distributed Intelligence | 2,3,5, 6,9,10, 13,16 | 1,3,4, 8,11 | 1,2,5, 6,8,13, 16 | 1,11, 13,16 | 1,2,8 | 1 |
| Modems | 3,5,9, 13 | 1,3,8, 11 | 1,13 | 1,11, 13 | 1 | 1 |
| Local loop | 3,5,9, 13 | 1,3,8 | 1,5,6, 7,13 | 1,7,11, 13 | | |
| Lines: dial-up, point-to-point, multipoint & loop | 3,5,9, 13 | 3,4,8, 17 | 5,6,7, 13 | 1,7,11, 13 | | |
| MUX/CONC/switch | 3,5,9 13,16 | 1,3,8 11 | 1,2,3, 4,5,6, 7,8,13, 16 | 1,7,11, 13 | 1,2,6, 8 | 1,2,6 |
| Front-end | 2,3,4, 5,9,10, 13,16, 17 | 1,3,8, 11 | 1,2,3, 4,5,6, 8,10, 13,16 | 1,7,13, 16 | 1,2,6, 8 | 1,2,6 |
| Computer | 2,3,4, 5,8,9, 10,13, 14,15, 16,17 | 1,3,4, 8,11 | 1,2,3, 4,5,6, 8,10, 13,16 | 1,7,13, 16 | 1,2,6, 8 | 1,2,6, 17 |

Table 1 (Concluded)

| Resources | Exposures | | | | | |
|---|---|---|---|---|---|---|
| | Errors & omissions | Disasters & disruptions | Loss of integrity | Disclosure | Defalcation | Theft of resources |
| Software | 3,4,5, 8,13, 15,16, 17 | 1,3,4, 11,15 | 1,2,3, 4,5,6, 8,10, 13,16 | 1,7,13, 16 | 6,8, 12,15, 16,17 | 1,2,6, 12,17 |
| People | 1,2,3, 4,6,8, 10,11, 13,14, 15,17 | 1,3,8, 11,12, 15 | 1,2,5, 6,8,11, 12,14, 15,16, 17 | 1,2,6, 8,12, 13,14, 17 | 1,2,6, 8,11, 12,17 | 2,14, 15,17 |

review each application system that is currently using the data communication network. The user is advised that there are some basic limitations that must be recognized. These limitations are as follows:

- The safeguards listed in the matrix are intended only as guidelines, not as standards, and should not be considered all inclusive with regard to a specific application system.
- The safeguards listed will assist in making a data communications system secure; it must be emphasized that security is relative, not absolute.
- Safeguards listed may not apply in all application situations, and, therefore, a general knowledge of data communications is assumed.
- The safeguards considered imply the state-of-the-art methods in use at the time (1977) this paper was written.

## 2. USE OF THE AUDIT MATRIX

To conduct a data communications security audit using the audit matrix, the auditor should first become familiar with the committee's definition of resources, exposures, and safeguards.

The auditor should then, for each resource utilized by each sensitive application on the system, follow a four-step procedure:

- Locate the resource on the left-hand vertical axis.
- Read across the row identifying each potential exposure.
- Consider each potential safeguard for applicability, given the specific application being run on the network.
- For each applicable safeguard, evaluate whether the current implementation of the safeguard is adequate.

The matrix can, additionally, be used to audit a general data communications system. The procedure, although basically unchanged, would be followed to evaluate system resources and exposures as they apply to the total system.

# 3. DEFINITION OF RESOURCES, EXPOSURES, AND SAFEGUARDS

## Resources

The following 10 resources are those resources that constitute an end-to-end data communications network (review Figure 1). This section defines each of the resources that are listed on the matrix (Table 1):

- Terminals--The devices used for input and/or output of computer recognizable information.
- Distributed Intelligence--The provision of capabilities for error detection and/or correction, authentication, message formatting, data validation and check sums, protocol, and any other logical and arithmetic function for validating the integrity of the data transmitted from the terminal.
- Modems--Modem is an acronym for MOdulator/DEModulator. The function performed is conversion of the data signals from a terminal to electrical forms acceptable for transmission on the particular communication links employed and vice versa.
- Local Loop--The communications facility between the customer's premises and the communications carrier central office. The local loop is assumed to be metallic pairs of wire.
- Lines--The common carrier facilities used as links in the communications network between central offices. These include terrestrial and satellite facilities.
  - Dial-Up: The switched telecommunication network and the various services provided therein, e.g., Toll, WATS, CCSA (Common Control Switching Arrangements).
  - Point-to-Point Private Lines: Dedicated leased facilities between two end points.
  - Multipoint or Loop Configured Private Line: Dedicated leased facilities shared among several (greater than two) end points.
- Multiplexor, Concentrator, and Switch--
  - Multiplexor: A device that combines, in one data stream, several data signals from independent end points.
  - Concentrator: An intelligent multiplexor.
  - Switch: A device that allows interconnection between any two lines connected to the switch.

- Front-End Processor--A device that interconnects the communications lines to the computer and performs a subset of the following functions:
  - Code and speed conversion
  - Protocol
  - Error detection and correction
  - Format checking
  - Authentication
  - Data validation
  - Statistical data gathering.
- Computer--An electronic data processing device referred to here only for its communications processing capability.
- Software--The instructions in the computer that cause the communications application processing functions to be performed.
- People--The individuals responsible for inputting data, operating and maintaining the equipment, writing the software, and managing the data communications environment.

## Exposures

The following six items depict the basic areas of exposure that are listed across the top of the matrix. This section defines the basic exposures to which a data communication network is subjected:

- Errors and Omissions--Inadvertent or naturally occurring problems excluding those resulting from deliberate or malicious actions. They include but are not limited to:
  - Inaccurate data
  - Incomplete data
  - Malfunctioning devices, lines, or software.
- Disasters and Disruptions (natural and manmade)--The destruction or temporary breakdown of the personnel or facilities required for the communication system to function. This results from natural and manmade disasters such as:
  - Common carrier breakdown.
  - Public utility breakdown.
  - Hardware/software breakdown.
  - The occurrence of a series of events each with low probability causing catastrophic loss.

- Loss of Integrity--The condition that exists when the system, including its hardware, software, data, and configuration is not in one of its intended states, i.e., it has been subjected to accidental, fraudulent or malicious action or destruction. Mere disclosure is not included in this definition. (Errors and omissions were treated separately in this matrix.)
- Disclosure--The unauthorized exposure of information.
- Defalcation--The intentional breach of the integrity of a system or its data by an individual or a group of individuals in a position of trust or performing their assigned tasks.
- Theft of Resources--The use of the facilities or services of a system for other than the intended purposes.

## Safeguards

The following 17 safeguards are the major categories of safeguards that an auditor should consider when reviewing the security of a data communication network. This section defines each safeguard. It should be noted that security measures applied to data communication networks can be costly. It is of great importance that a realistic and pragmatic evaluation be made of the potential threat as well as the possible safeguards for countering the threat to ensure a cost effective application of these safeguards. The auditor should conduct a threat assessment with regard to a potential loss of the application involved, the probability of that loss, and the cost of providing an adequate safeguard:

(1) Physical Security Controls--The use of locks, guards, badges, sensors, alarms and administrative measures to protect the physical facilities, computer, data communications, and related equipment. These safeguards are required for access monitoring and control for and the physical protection of the computer and to protect data communications equipment from damage by accident, fire, and environmental hazard, both intentional and unintentional in nature. These safeguards are employed to detect, deter, prevent, and report security exposures. Audit consists of determination of existence of specific physical security measures, effectiveness of their functioning, and testing of reliability.

(2) Audit Trails--A chronological record of system activities that is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to each event. Selected journals or reports include:

- Computer log-on/log-off
- Physical access log-in/log-out

- Resource allocation and use
- Reconciliation of inputs to outputs
- Frequency of specific events
- Forward and backward tracing
- Network utilization.

This safeguard is employed to detect, recover, correct, or report security exposures. Audit consists of determination of reasonableness, completeness, and scope.

(3) Back-up--The availability and protection of resources to be used to replace or duplicate those used in normal operation. This includes operational and written procedures for regular review, update, and testing of back-up resources. This safeguard is employed to prevent loss, and to correct or to help recover from errors. Audit should determine appropriateness of backup techniques for risk involved.

(4) Recovery Procedures--The actions, procedures, or systems used to restore resources to normal operational capability in a timely, cost-effective manner. Audit should determine workability or feasibility of recovery procedures.

(5) Error Detection/Correction--The techniques, procedures, or systems used to detect and correct errors by methods such as echoing, forward error correction, and automatic detection and retransmission methodologies. This may involve validation through selective algorithms, parity checks, check sum, etc. This safeguard is used to detect and correct errors. The auditor should determine limitations of techniques, procedures, or systems.

(6) Authentication--The act of identifying or verifying the identity, authenticity, and eligibility of a terminal, message, user, or computer. Authentication devices are used to detect, prevent, and deter exposures. These include but are not limited to:

- User passwords
- Keys
- Badges
- Message sequencing
- Terminal/computer call back
- Network protocol
- Encryption.

The auditor should determine existence and completeness of the safeguards.

(7) Encryption--Transformation of data to hide its original contents or prevent its undetected modification. The considerations are:

- Specified precisely to meet some standard, e.g., the NBS Data Encryption Standard.
- Matched to vulnerabilities and characteristics of the communication system and the data involved.
- Various ways to encrypt, e.g., link-by-link or end-to-end.
- Requires administrative procedures to select keys to be used, dictate when to change them, and control their distribution.
- Integrate into system design in future applications when justified by the appropriate cost/risk analysis.
- Add communications overhead to distribute keys, initialize and synchronize devices, and recover from communications errors.

Auditor should first evaluate vulnerabilities of system and data, review the objectives of the encryption system, and then measure the effectiveness of the physical and administrative procedures supporting encryption.

(8) Operational Procedures--The administrative regulations, policies, and day-to-day activities supporting the security safeguards of a data communication system such as:

- Specification of the objectives of ADP security for an organization, especially as they relate to data communications.
- Planning for contingencies of security "events," including recording of all exception conditions and activities.
- Assure management that other safeguards are implemented, maintained and audited, including background checks, security clearances and hiring of people with adequate security-oriented characteristics; separation of duties; mandatory vacations.
- Develop effective safeguard for deterring, detecting, preventing, and correcting undesirable security events.
- Cost effective, often resulting in related benefits such as better efficiency, improved reliability, and economy.

Auditor should look for the existence of current administrative regulations, security plans, contingency plans, risk analysis, personnel understanding of management objectives, and then review the adequacy and timeliness of the specified procedures in satisfying these.

(9) Preventive Maintenance--Scheduled diagnostic testing: cleaning, replacement, and inspection of equipment to evaluate its accuracy, reliability, and integrity. This includes:

- Develop schedules for testing and repair.
- Ensure that maintenance personnel are given the time and resources to deter or prevent failures of equipment.
- Keep inventory of replacement parts, based on failure statistics, such as Mean Time Between Failure (MTBF) for each device.
- Keep maintenance records and analyze them for recurring problems or statistically unexpected security exposures.
- Perform unscheduled replacement or testing for specific devices to detect unauthorized modification ("bugging," etc.). This reduces the likelihood of failures during critical periods and, as a by-product, detects unauthorized modification of resources.

Auditor should review maintenance schedules, records, inventory of parts, "downtime," cost-to-repair-or-replace charts, and compare these with those of similar systems.

(10) Format checking--A method of verifying data as being reasonable through checks and balances. Develop automated verification system to detect data entry errors using methods such as range checking (numerical fields), record counts, alphabetic characters in numeric fields, field separators, etc.

Auditors should evaluate areas where format checking can be used and verify that adequate checks are made.

(11) Insurance--Financial protection against major losses. Insurance is used to share a potential or actual loss and to protect against or recover from major disasters by budgeting resources over the long term.

Auditors should evaluate whether protection may be more easily obtained from alternative safeguards, and that major catastrophies will not expose the organization to unacceptable risks.

(12) Legal Contract--An agreement for performing a specific service on a specific costing basis, generally incurring specific liability. Examples include bonding, conflict of interest agreements, clearances, nondisclosure agreements, and the like. Other examples include:

- Agreements establishing liability for specific security events.
- Agreements not to perform certain acts or a penalty will be incurred.

Auditor should review the legal document for adequacy and protection afforded.

(13) Fault Isolation/Diagnostics--The techniques used to ascertain the integrity of the various hardware/software components comprising the total data communications entity. These techniques are used to audit the total environment and to isolate the offending elements either on a periodic basis or upon detection of a failure. These techniques include:

- Diagnostic software routines
- Electrical loopback
- Test message generation
- Administrative and personnel procedures.

Auditor should review the adequacy of the techniques used for fault isolation.

(14) Training/Education--Training and education of employees serves both to aid in preventing problems and in correcting them when they have occurred. It serves to clearly define responsibility and to familiarize employees with accepted procedures.

Auditor should review ongoing educational policies.

Education also includes training in the whys--including why security and controls are important to the organization. The potential repercussions of a failure and the need to follow procedures or observe controls should also be addressed.

Auditor should ensure that management is aware of the need and advantages of education and that training is used on a continuing basis.

(15) Documentation--Documentation is a precise description of programs, hardware, system configuration, and procedures intended to assist in prevention or problems, identifying the causes of problems, and recovering from the problems. It should be sufficiently detailed to assist in reconstructing the system from its parts.

Auditor should determine that documentation exists to the extent required to meet reasonable anticipated needs.

(16) Testing--The techniques used to validate the hardware and software operation to ensure integrity. Testing, including that of personnel, should uncover departures from specified operation.

Auditor should determine that testing exists to the extent required.

(17) Reporting and Statistics--The gathering and reporting of information which defines the usage of all facets of the data communications entity. The generation of exception reports for management including:

- Traffic statistics
- Maintenance statistics
- Error performance
- Terminal usage by time and activity.

Auditor should determine that reporting and statistics exist to the extent required to meet future planning needs.

# PART XI: POST-PROCESSING AUDIT TOOLS AND TECHNIQUES

Chairperson: Richard D. Webb
Touche Ross & Company

Participants:

Leo Deege
  Defense Audit Service
Philip M. McLellan
  Royal Canadian Mounted Police
Albrecht J. Neumann, Recorder
  National Bureau of Standards
Michael J. Sopko
  GTE Service Corporation
Norman Statland
  Price Waterhouse & Company
Robert Stone
  Uniroyal Corporation

From left to right: Richard D. Webb, Philip M. McLellan, Zella G. Ruthberg (visiting Vice Chairman), Robert Stone, Leo Deege, Michael J. Sopko, Albrecht J. Neumann

---

Note: Titles and addresses of attendees can be found in Appendix A.

## EDITORS' NOTE

A breif biography of the Session Chairperson follows:

Mr. Richard D. Webb is a Manager in the Executive Office of Touche Ross & Company. He is responsible for research and development of EDP audit policies, EDP audit techniques, and EDP audit training. He had significant responsibilities on the EDP audit team that investigated the Equity Funding situation for the Trustees in Bankruptcy. He has designed and implemented audit software packages and has been a financial and cost accounting systems consultant. Mr. Webb is a Certified Public Accountant (IL) and a member of the American Institute of Certified Public Accountants where he is Chairman of the Audit Software Specifications Task Force; a member of the Computer Audit Subcommittee; and a member of the Computer Audit Techniques and Approaches Audit Guide Project Team. He was also a member of the task forces that drafted the AICPA audit guides entitled, "Audits of Service Center Produced Records" and "Auditor's Study and Evaluation of Internal Controls in EDP Systems." He is a member of the Board of Directors of the New York Chapter of the EDP Auditor's Association and a member of the New York Society of CPAs. Mr. Webb received his BS in accounting from the University of Minnesota.

The charge given to this session was:

> POST-PROCESSING AUDIT TOOLS AND TECHNIQUES: What are the post-processing audit tools and techniques available or needed for the effective use of the various system journals and logs in an audit of computer security?

Many different logs and journals are produced, or can be produced, that provide important information to the auditor evaluating computer security. Two of the major problems that the auditor often encounters are the overwhelming volume of information and inadequate analytical tools.

This session is to consider the type of information needed, the most effective and efficient method of capture, and the tools and techniques required for analysis. Consideration should be given to what tools are currently available as well as those needed to be developed.

The following is a consensus report initially reviewed by the entire group.

# POST PROCESSING AUDIT TOOLS AND TECHNIQUES

by

A. J. Neumann
N. Statland
R. D. Webb

## 1. INTRODUCTION

This paper summarizes the discussions and conclusions of the session dealing with post processing audit tools and techniques. The group consisted of a mix of external and internal auditors, security specialists and computer oriented generalists. Early in the deliberations it was agreed upon to develop and adhere to an outline, to discuss some basic definitions, and to agree on a scope for a security audit.

Based on a common understanding of the scope of the problem, we agreed to look at available data by dividing the total system into system access, input, processing , and output areas. We would attempt to determine typical security audit information requirements; i.e. what information would an auditor need in the post-processing environment to perform a security audit, and what information might be needed that is usually not available in today's environment. Next we would assess existing tools and techniques, and identify needed techniques.

The authors wish to acknowledge many contributions made during the Miami meetings and constructive comments made during the review of several draft versions of this paper by L. Deege, P. M. McLellan, R. Stone, and M. J. Sopko. H. Robinson arranged the original session but was, however, unable to attend because of a last minute emergency. He did however contribute to drafts of this paper.

## 2. OBJECTIVES OF A TYPICAL SECURITY AUDIT

The post processing activities of the auditor are presented here in the context of a security audit and include confidentiality, integrity and availability of data. They also include the degree of compliance with approved procedures. Our discussion was intended to encompass environments ranging from those requiring very little security, to environments at the National Security level. Also, the context of the discussion does not specifically address or exclude audits where the objective is an opinion on: the financial statements; system efficacy; system efficiency; or whether the results of the system are used effectively.

General objectives of such a security audit were agreed to be the determination of the existence, scope and adequacy of controls in light of the level of information protection required by the nature of the system.

Several specific objectives were noted:

a. Determine that all transactions were completely processed and that they were processed once and only once. (uniqueness of transactions).

b. Determine that each transaction is complete, accurate and authorized. (completeness, accuracy, and authorization controls for transactions, i.e. transaction integrity).

c. Determine that processing was complete, accurate, and authorized. (completeness, accuracy, and authorization controls of processing, i.e. processing integrity).

d. Determine that distribution of processing results was made only to authorized recipients. (distribution control).

e. Determine that data and the required use of system resources were recoverable. (recoverability control).

f. Determine the ability to detect and analyze security violations. (detection and analysis capability, i.e. violation control).

It was understood that the auditor would have to first "understand the system" being audited in order to work towards the stated objectives. Discussion of security audit led to formulation of the following definitions.

## 3. DEFINITIONS

Computer Security — The protection of system data and resources from accidental and deliberate threats to confidentiality, integrity, and availability.

Computer Security Audit — An examination of computer security procedures and measures for the purpose of evaluating their adequacy and degree of compliance with established policy.

Note: This definition covers computer security, rather than data security, which is included in the broader concept. It was felt that the definition of security audit in FIPS PUB 39 dealing with data security only should be broadened to the definition given here.

Post Processing Audit — The post-facto analysis of input, processing, and output information for the purpose of validating compliance with pre-determined system requirements including those for security.

Log — A chronological record of data elements representing specified actions taken for specific purposes during system operation. "Data element" is used here in its broadest sense to include application data as well as system performance related data etc.

Tools vs. Techniques — A technique is a method of accomplishing a desired objective; thus a technique may consist of procedures that contain several tools, or a technique may employ several tools alternately. For example audit software is a tool that can be used in many techniques.

Transaction — A collection of data about an event. It may be processed or rejected, but from an auditor's viewpoint should always be recorded. The term is used here in its broadest sense from an operator action at a terminal served by a computer to a financial transaction or a textual message.

## 4. SCOPE OF POST PROCESSING AUDIT

While the scope of a post processing audit extends beyond the EDP system proper and includes review of manual and automated controls, this discussion deals only with techniques and tools covering the EDP system proper. That is the audit covers processing of transactions from the time of initial conversion of data through intermediate processing stages and telecommunications to the delivery of output. The mode of processing (that is, on-line vs. batch) was not considered to be a limiting factor, though several of the logs discussed may be appropriate only in one or the other mode. The auditor is assumed to have sufficient knowledge of systems to be able to judge the impact of system performance on security and also to effectively review manual areas prior to conversion and subsequent to output. Figure 1 shows in diagrammatic form the scope of post-processing security audit.

## 5. INFORMATION REQUIREMENTS

Achievement of the objectives of a security audit generally requires information about the following areas: ACCESS, INPUT, PROCESSING and OUTPUT. The auditor should review each of the areas and look for information detail in a log showing the following five basic types of information labelled : WHO, FUNCTION, WHAT, STATUS, and TIME. (These are illustrated in tables 1 through 4).

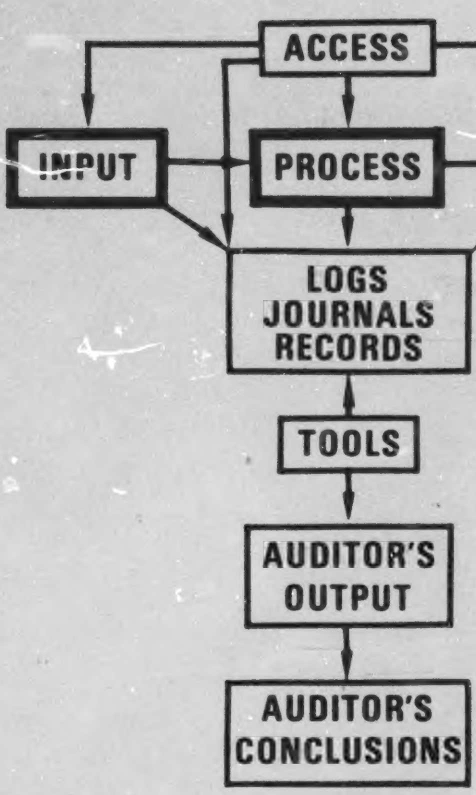


FIGURE 1. POST PROCESSING SECURITY AUDIT

## TABLE 1: SYSTEM LOG ACCESS INFORMATION

| WHO | FUNCTION | WHAT | STATUS | TIME |
|---|---|---|---|---|
| USER ID | ENTRY | SYSTEM ID & DEVICE ID | SUCCESSFUL/ UNSUCCESSFUL | D–T |
| USER ID | EXIT/ RELEASE | SYSTEM ID & DEVICE ID | " | D–T |

D=DATE
T=TIME

## TABLE 2: INPUT LOG INFORMATION

| WHO | FUNCTION | WHAT | STATUS | TIME |
|---|---|---|---|---|
| TASK ID | REQUEST TO OPEN FOR READ | RESOURCES I.E. FILES, DEVICES, PROGRAMS DATA | SUCCESSFUL/ UNSUCCESSFUL | D–T |
| TASK ID | READ | FILE, DATA ELEMENTS | " | D–T–SN |
| USER ID | ENTER | TASK ID | " | D–T |

D=DATE SN=SERIAL #
T=TIME

## TABLE 3: PROCESSING LOG INFORMATION

| WHO | FUNCTION | WHAT | STATUS | TIME |
|---|---|---|---|---|
| TASK ID | VALIDATE | TRANSACTION TYPE CONTENT | N/A | N/A |
| TASK ID | FORMAT LOG RECORD | TRANSACTION | VALID/ INVALID | D–T–SN EACH TRANSACTION |
| TASK ID | COUNT & SUMMARIZE | " | N/A | N/A |
| TASK ID | FORMAT LOG RECORD | TASK COUNTS & SUMS | N/A | D–T–SN |
| TASK ID | UPDATE | MASTER | N/A | N/A |
| TASK ID | SAVE | MASTER FILE LOG | NORMAL/ ABNORMAL | D–T–SN OF TRANSACTION |
| TASK ID | SAVE | PERIODIC BACKUP FILE | N/A | D–T–SN |
| TASK ID | COUNT & SUMMARIZE | DATA BASE LOGICAL FILE FOR EACH TASK | N/A | D–T–SN |

D=DATE SN=SERIAL #
T=TIME

## TABLE 4: OUTPUT LOG INFORMATION

| WHO | FUNCTION | WHAT | STATUS | TIME |
|---|---|---|---|---|
| TASK/ USER ID | REQUEST WRITE (UPDATE) | FILE ID<br>DEVICE ID | SUCCESSFUL/ UNSUCCESSFUL<br>DEVICE/STATUS CHANGE | D–T |
| TASK ID | WRITE (UPDATE) | DEVICE ID<br>FILE ID<br>MACHINE OR HUMAN READABLE | COMPLETE/ INCOMPLETE | D–T |

D=DATE
T=TIME

WHO identifies the cause or initiating force of a transaction. The cause may be a person or a process, manual tasks, or a program.

The FUNCTION is descriptive of a processing action such as "entry", "request to read", "validate", "count" etc.

The items labelled WHAT identify objects of the processing action. They may be files, devices, programs, or data elements.

The STATUS information refers to the function and the associated cause and objects. An action may be complete or incomplete, correct or incorrect, etc.

TIME provides a date-time stamp associated with the recorded action and status. It provides basic time information which can be used to determine audit trails, and in general to trace system continuities. In some cases a transaction or record serial number will be associated with a date time stamp.

Tables 1 through 4 show typical information requirements in tabular form. These tables are not all inclusive and should not be considered complete in any way. They do illustrate a train of thought, and indicate a methodology which could be used to check security information requirements available in existing systems, and those to be specified for future systems. No time sequence is to be implied by the position of the rows in the various tables. Each line in these tables forms a basic record of information pertaining to security, which may be recorded or logged and then processed at a later time for security audit purposes.

## 6. TYPICALLY AVAILABLE INFORMATION

In most existing systems a variety of information is available for post-processing audits. A variety of logs are prepared routinely for accounting purposes, system maintenance and for system performance monitoring. A console log may routinely record and print out coded system malfunctions in terms of error messages and times of occurrence. An event log might also record terminal ID and user ID of successful system entries. It may also record unsuccessful entries and associated passwords used on that occasion. Every user command, the time of the command, and terminal and user ID may also be logged. From an EDP department accounting standpoint there should be records of the program or job run, the various measures used in billing (connect time, CPU time, resource units etc.), the user or organization ID, etc. Some of this information is useful for security audits.

Security related information should include time of action, type of action, record of unauthorized passwords used, resource control, and other means used in the violation.

## 7. ILLUSTRATIVE EXAMPLE: ELECTRONIC FUNDS TRANSFER SYSTEM

The next paragraphs illustrate security information requirements in the context of an electronic funds transfer system. Figure 2 shows a system block diagram, major system components, and various logs used for security purposes. A number of retail terminals are connected to a regional communications controller. Several of these controllers may be connected to bank computers or to each other. Records and logs are maintained at the communication controllers and at central bank computers.

The controller maintains a reference log and a journal. Four major software functions are postulated for the central computer: the operating system, and the input, processing and output functions. All of these maintain appropriate logs and records for security purposes.

### 7.1 Remote Terminal Procedures

Procedures at the remote terminal are designed to build up security information in the various logs. A customer is identified by a personal identification number to restrict access to appropriate file segements. A transaction type may be entered, which permits validation of the terminal use for the particular type of transaction. A further check may be made on the terminal identification, which may be hard wired. Additional authorization codes may be required to permit credit operations, adjustments i.e. returns, and high value debit transactions. Each acknowledgment of a transaction is identified with a sequence number, which is generated in the terminal.

### 7.2 Message Security at the Switching Computer.

Messages are formatted into message headers and the message content.

7.2.1 Message Headers. A header usually will contain the following information:

Originating terminal ID
Message type designator
Priority code
Message sequence number (assigned at each terminal)
Routing indicator
Message character count

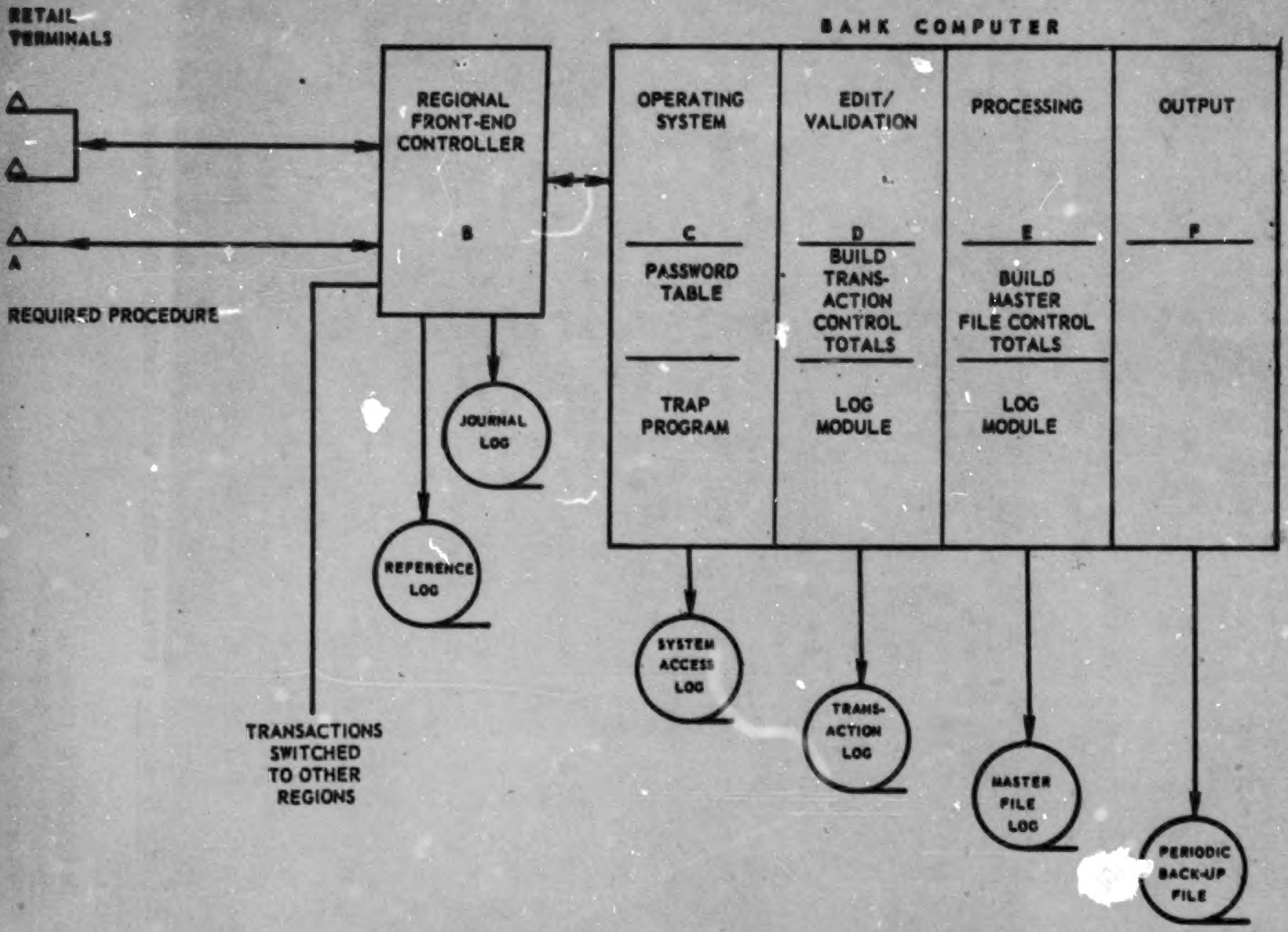


FIGURE 2. SECURITY CONSIDERATIONS WITHIN EFTS SYSTEM ARCHITECTURE

7.2.2 Message acknowledgment and release. After validation of the message character count, the switching computer is accountable for each message until the the receiving unit e.g a terminal, host computer or another switching center acknowledges receipt of the message. If message count, origin or destination codes are invalid, retransmission is requested, using the same message sequence number.

7.2.3 Ledger balancing. By maintaining a list of input and output actions for each message, ledgers are maintained in a continuous state of balance.

### 7.3 Communications Processor Logs

All message header data are maintained on the reference log, while message contents are stored on the journal log.

### 7.4 Bank Computer Functions and Logs

The input function primarily deals with validation and editing of the transactions. A transaction log is maintained. The operating system maintains a system access log, the processing function maintains a master file log, while the output module maintains periodic back up files, which may be used during system failures to reconstitute records and files. Table 5 shows data required by the system log. Sign-on and file entry would require use of encrypted passwords with associated indicators showing which files, devices, programs may be used. Table 6 shows data requirements for editing and validating of input transactions, while tables 7 and 8 show data requirements for processing and updating, and for output.

## 8. POST PROCESSING TECHNIQUES

Several post-processing techniques were identified by the working group. They are presented here by area and without guidelines for use in specific circumstances since use of a specific technique would require the auditor to consider several factors such as timing and cost.

### 8.1 ACCESS

8.1.1 Unsuccessful accesses. List all unsuccessful accesses by level of security in order to determine who accessed, and why attempt was unsuccessful. Determine frequency and quantity. Determine characteristic patterns and compare to authorization table. This would aid in detection of unauthorized users.

## TABLE 5: OPERATING SYSTEM— SECURITY ACCESS CONTROL LOG DATA

| WHO | FUNCTION | WHAT | STATUS | TIME |
|---|---|---|---|---|
| SUBSCRIBER ID | SIGN-ON | SYSTEM DEVICE ID | SUCCESSFUL/ UNSUCCESSFUL | D–T |
| SUBSCRIBER ID | RELEASE | SYSTEM DEVICE ID | SUCCESSFUL/ UNSUCCESSFUL | D–T |
| SUBSCRIBER ID | ENTER | TASK ID<br>TRANSACTION TYPE | SUCCESSFUL/ UNSUCCESSFUL | D–T |
| TASK ID | REQUEST TO USE (ACCESS FOR READ) | RESOURCES I.E. FILES, DEVICES, PROGRAMS, JCL PROCEDURES | SUCCESSFUL/ UNSUCCESSFUL | D–T |

COMPLETION OF TASKS 1&3 WILL REQUIRE USE OF A STORED, ENCIPHERED PASSWORD WITH ASSOCIATED INDICATORS OF WHICH FILES, DEVICES, PROGRAMS, ETC. THIS TASK MAY USE

D=DATE
T=TIME

A "TRAP" PROGRAM SHOULD BE USED TO NOTE OCCURRENCE OF UNUSUAL TRAFFIC PATTERNS.

## TABLE 6: SECURITY REQUIREMENTS DURING EDIT/VALIDATION OF INPUT TRANSACTIONS

| WHO | FUNCTION | WHAT | STATUS | TIME |
|---|---|---|---|---|
| TASK ID | VALIDATE | TRANSACTION CONTENT | N/A | N/A |
| TASK ID | FORMAT/ WRITE LOG RECORD | TRANSACTION | VALID/ INVALID | D–T– TRANSACTION SN (INCLUDING TERMINAL) |
| TASK ID | COUNT & ADD TO CONTROL TOTALS MAINTAINED FOR EACH TERMINAL BY TRANSACTION TYPE | TRANSACTION & SELECTED DATA ELEMENTS | N/A | N/A |

D=DATE T=TIME SN=SERIAL #

## TABLE 7: SECURITY REQUIREMENTS DURING PROCESSING/UPDATE OF DATA

| WHO | FUNCTION | WHAT | STATUS | TIME |
|---|---|---|---|---|
| TASK ID | UPDATE | MASTER FILES | N/A | N/A |
| TASK ID | SAVE | MASTER FILE BEFORE/AFTER IMAGE ON LOG | NORMAL/ ABNORMAL | D–T– TRANSACTION SN |
| TASK ID | COUNT & ADD TO CONTROL TOTALS | MASTER FILE RECORDS SELECTED DATA ELEMENTS | N/A | D–T– MASTER FILE VN |

D=DATE SN=SERIAL #
T=TIME VN=VERSION #

## TABLE 8: SECURITY REQUIREMENTS DURING OUTPUT OF DATA

| WHO | FUNCTION | WHAT | STATUS | TIME |
|---|---|---|---|---|
| TASK ID | FORMAT SUMMARY RECORDS FOR TRANSACTION & MASTER FILE LOGS | RECORD COUNTS & CONTROL TOTALS OF SELECTED DATA ELEMENTS | N/A | D–T–SN–VN |
| TASK/ USER ID | REQUEST WRITE/ UPDATE | FILE ID<br>DEVICE ID | SUCCESSFUL/ UNSUCCESSFUL DEVICE STATUS | D–T |
| TASK ID | WRITE/ UPDATE-IN-PLACE | DEVICE ID<br>FILE ID<br>FOR MACHINE OR VISUAL READ | COMPLETE/ INCOMPLETE | D–T |
| TASK ID | WRITE | PERIODIC BACKUP FILE | N/A | D–T–SN–VN |

D=DATE SN=SERIAL #
T=TIME VN=VERSION #

8.1.2 Successful accesses. List all successful entries to determine usage patterns. Compare successful entries to authorization table.

8.1.3 Log continuity check. Establish a log continuity check to determine when the system did not indicate that it was in use and check against processing schedule. All unscheduled breaks in system activity should be explained.

## 8.2 INPUT

Techniques 1, 2, 3 apply as shown in ACCESS.

## 8.3 PROCESSING

Here a variety of techniques can be used to check processing integrity and security .

8.3.1 Manual Checking. Manual checking of a selected set of previously processed transactions can be used to verify results produced in an actual, previous processing cycle.

8.3.2 Control Totals. Independent determination of the control totals of actual files by means of audit programs permit checking of totals against reported totals produced by the system.

8.3.3 Test Data. System test data can be used to produce control totals or results that are to be checked against predetermined totals. (base case / test decks )

8.3.4 Integrated Test Facility. Here the auditor selects special transactions to be processed against auditor controlled file segments or records. This method is used frequently to test selected processing paths of on-line processing systems. This may be done on a regular or unscheduled basis, and provides a deterrent to fraud since the ITF may be designed to be transparent to programming and operations personnel. They would thus not be aware of ongoing security audit testing.

8.3.5 Tagging. Tagged transactions(i.e. transactions to which special codes have been assigned by the auditor) can be traced through the processing of live production runs, in order to examine intermediate processing results.

8.3.6 Extended Record Maintenance. Extended record maintenance can be used to add and maintain transaction records within a master file, that can be used to provide the processing history of a master file. In-line data collection provides samples of data, or stratification as an extension of the application program.

8.3.7 Tracing. Tracing can be used to document use of program modules, or program instructions to process specific transactions. It is used to verify process logic and to identify unused portions of computer programs.

8.3.8 Mapping. Use of program analyzers permits mapping of all object program modules included in the load image library to determine what special conditions lead to the execution of each program module.

8.3.9 Recompilation. Recompilation of the source statement version of the program, and processing of the resultant object code against a recent set of transactions can be done. A comparison of the two sets of results may lead to evidence of improper processing. Additionally the current source program can be recompiled with the resulting object module mechanically compared to the current production module resident in the library. This technique would identify modifications to the object module not reflected in the source code. Once the source code logic has been proven, an auditor controlled copy could be maintained for subsequent comparison with the production version to detect program modifications.

8.3.10 Parallel simulation. Parallel simulation programs using selected application logic, calculations and controls, relevant to specific auditing tests can be used to reprocess selected actual transactions. Critical calculations can be verified by processing in another language. Depending upon system complexity and the degree of flexibility available, a generalized software package could be used to parallel the operation of a system.

8.3.11 Retrieval Programs. Record retrieval programs can be used to select transactions that either meet specified selection criteria, or are selected as a result of statistical sampling criteria. Printed reports can be produced which can be used for further analysis and investigation.

## 8.4 OUTPUT

The following post-processing techniques are used in checking system output.

8.4.1 Output Listing. List the outputs and verify disposition of output, including schedule compliance.

8.4.2 Authorization Listing. List authorizations (as in input).

The post-processing techniques listed in the previous paragraphs have been summarized and related to the security audit objectives in Figure 3. It appears that fewer techniques are available for distribution control, recoverability and violation control, than for uniqueness and integrity of transactions and of processing.

| | SECURITY AUDIT OBJECTIVES | | | | | |
|---|---|---|---|---|---|---|
| TECHNIQUES | UNIQUENESS | TRANSACTION INTEGRITY | PROCESSING INTEGRITY | DISTRIBUTION CONTROL | RECOVERABILITY | VIOLATION CONTROL |
| MANUAL CHECKING | ● | ● | ● | | | |
| CONTROL TOTALS | ● | | ● | | | |
| TEST DATA | ● | ● | ● | ● | ● | ● |
| INTEGRATED TEST FACILITY | ● | ● | ● | ● | ● | ● |
| TAGGING | ● | ● | ● | | | |
| EXTENDED RECORD MAINTENANCE | ● | ● | ● | | ● | |
| TRACING | | ● | ● | | | |
| MAPPING | | ● | ● | | | |
| PROGRAM ANALYZER | | | ● | | | |
| RECOMPILING | | | ● | | | ● |
| SIMULATION | ● | ● | ● | | | ● |
| RECORD SELECTION | ● | ● | ● | | | ● |

FIGURE 3. TECHNIQUES IN SUPPORT OF AUDIT OBJECTIVES

## 9. NEEDED TECHNIQUES

Techniques could be developed or improved in two areas, those of logging security audit data, and analysis and manipulation of the logs.

### 9.1 Logging methods

Security of the security log needs to be established. Security data should be considered for encryption, i.e. passwords and critical logs should be protected from unauthorized access.

Security logs can be established using one or more of the following methods:
The simplest method would be to use the present operating system software. This would provide only minimal protection because it is dependent on the operating system and the people who control it.

A special purpose device, i.e. a tamper proof, secure, recording microprocessor, actuated by special instructions contained in all programs could also be used. Such a device would record all activity, including use of special control programs (e. g. "super-zap"), that normally leave no trace on the systems log. Similarly such a device could record all calls to program libraries.

A complete hardware monitor similar to a cockpit flight recorder with probes at critical control points throughout the system is another alternative. It could provide a complete security log, with a proper level of protection, independent of the system being monitored.

### 9.2 Software Tools

It was the consensus of the group that much can be done with existing techniques, and that no new techniques needed to be developed.

Existing audit software could be made easier to use, and degrees of improvement could be made. Also existence of software capabilities needs to be publicized,— many auditors do not know "what" is available "where".

Available tools appear to be too cumbersome to use, and often are primitive. For example, certain procedures described earlier, though having common objectives, generally require complicated programming to accomplish their goals using today's tools. Higher level software to access logs for audit purposes could be developed.

Elements in the various tools are often not coordinated, e.g. tracing and mapping . These techniques are generally appropriate to be used together, and facilities could be developed so that they could be used together.

## 10. CONCLUSIONS AND RECOMMENDATIONS

Information should be published for the benefit of auditors on "what" audit tools are available "where". That is, a catalog of tools for security audit should be developed. This catalog would provide details of components, and would be indexed according to techniques, hardware, and software required to use the tools. Comments about the level of difficulty would also be included.

Security log data should be built into new systems during their development. Security oriented personnel should paticipate in planning, development and design of systems, to insure auditability.

Secure logging hardware components should be explored, to provide tamper-proof recording capability for security audit purposes.

## 11. REFERENCES

1. Computer Control and Audit.
   William C. Mair, Donald R. Wood, Keagle W. Davis.
   The Institute of Internal Auditors, Inc.
   Second Edition Revised and Enlarged, 1976.

2. Features of Seven Audit Software Packages--
   Principles and Capabilities. A. J. Neumann .
   Special Publication NBS 500-13.
   National Bureau of Standards, July 1977.

3. Management Controls for Data Processing.
   International Business Machines Corporation.
   GF 20-0006-1, Second Edition, April 1976.

4. Stanford Research Institute,
   Systems Auditability and Control Study,
   -Executive Report.

## PART XII: INTERACTIVE AUDIT TOOLS AND TECHNIQUES

Chairperson: Hart J. Will
University of British Columbia

Participants:

Robert P. Blanc
National Bureau of Standards
Henk Brussel
University of British Columbia
Peter S. Browne, Recorder
Computer Resource Controls

Robert S. Roussey
Arthur Andersen & Company
Joseph J. Wasserman
J. J. Wasserman & Company
Donald R. Wood
Touche Ross & Company

From left to right: Robert P. Blanc, Donald R. Wood, Peter S. Browne, Jospeh J. Wasserman, Hart J. Will, Robert S. Roussey, Robert V. Jacobson (visiting session coordinator), Henk Brussel.

---

Note: Titles and addresses of attendees are in Appendix A.

## EDITORS' NOTE

A breif biography of the Session Chairperson follows:

Dr. Hart J. Will has been on the Faculty of Commerce and Business Administration at the University of British Columbia since 1969, first as Assistant Professor and currently as Associate Professor of Accounting and Management Information Systems. His teaching and research interests lie in: MIS analysis, design, audit, control and security; data base management and administration; and audit software in general and ACL (Audit Command Language) in particular. He has worked, consulted, taught, and published extensively in Europe and North America. His activities include: Chairman of U.E.C. International Symposium on Computer Auditing: Legal and Technical Issues, St. Augustin, Germany: GMD, June 18-20, 1975 and Editor of Legal and Technical Issues of Computer Auditing, the Conference Proceedings; visiting Research Professor, Gesellschaft fuer Mathematik and Datenverarbeitung (GMD), St. Augustin, Germany 1974-75; founding chairman of an informal DBMS Workshop, 1976-77; and currently Associate Editor of INFOR, Canadian Journal of Operational Research and Information Processing 1977. His degrees are; Diplom-Kaufmann (Free University Berlin), Ph.D. (University of Illinois at Urbana-Champaign).

The charge given to this session was:

> INTERACTIVE AUDIT TOOLS AND TECHNIQUES: What are the interactive audit tools and techniques available or needed to permit on-line auditing of computer security?

The Institute of Internal Auditors considers internal audit a managerial control which functions by measuring and evaluating the effectiveness of other controls. It has become increasingly difficult in an ADP environment for the auditor to fulfill this responsibility in a responsive way and continue to audit on an after-the-fact basis. The speed of processing alone requires a different approach.

This session is to explore the audit tools and techniques that can be applied today and those that are needed to be developed which will permit on-line evaluation of data integrity.

The consensus report that follows was developed and reviewed by the entire membership of this session.

# Interactive Audit Tools and Techniques
# A Group Concensus Report

Hart J. Will and group members

## 1. EXECUTIVE SUMMARY

### 1.1 Introduction

### 1.1.1 Interactiveness

In an audit context, interactiveness is usually interpreted as on-line coding of audit programs, although the interactive audit programming feature is available only in relatively few systems. Another dimension of interactiveness is on-line audit processing in a human-machine dialogue in terms of free-format audit investigations of a computerized information system. In regard to computer security, some use has been made of gathering on-line system performance information (SMF, time-sharing session data, etc.) for purposes of near real-time monitoring and control. Yet in a computer communications system which is itself highly interactive and where use of data base technology is predominant, the requirements exist for increased capability to use the computer also as an interactive audit tool.

### 1.1.2 Research and Development

There are many existing computer audit tools and techniques that are being used on a partially interactive basis. Interactiveness is desirable in the development and maintenance of performance. The working group believes that research and development is needed with respect to true interactive tools and techniques. The report includes some examples of possible areas for further study.

### 1.1.3 Subject Areas

The following subjects are of interest to the group:

- Interactive use of existing audit tools and techniques to increase audit efficiency.
- Development of new tools and techniques in order to facilitate the performance assurance process in general and auditing in particular.
- Development and use of techniques to increase the auditability of computer systems.

### 1.2 Summary

### 1.2.1 Performance Assurance

The summary framework is that of performance assurance, which is defined as the assurance that a computer system is performing its intended functions within a specified degree of accuracy, timeliness, and data security, and that it is not performing unintended functions. Performance assurance is the domain of several different kinds of people and include the Certified Public Accountant, senior organizational management, internal auditors, the quality assurance function and operational management. Basic definitions and objectives are covered in section 2. Section 3 describes the performance assurance function in terms of four activities:

- Project control objectives
- Information gathering
- Analysis and evaluation
- Testing

### 1.2.2 Existing Tools and Techniques

Existing tools and techniques that can be used interactively are discussed in section 4.

### 1.2.3 Needed Tools and Techniques

Additional needed performance assurance tools and techniques that should be quite useful in the detection of malfunctions of systems procedures or control are discussed in section 5. It is possible to identify symptoms relating to data or program errors, anomalous activity, access control breaches and any activity that exceeds pre-determined thresholds. The following categories of tools measure these symptoms:

- Near real-time error detection and correction.
- Monitoring of adequacy of controls.
- Measurement of design accuracy.
- Program modification control.
- Monitoring of system troubles or activity.

## 1.3 Use of Interactive Tools and Techniques

The working group has identified two major categories of uses for interactive computing. They are interactive audit programming and interactive audit processing. These are defined in section 2 of the report. In the case of interactive audit programming, the benefits to the auditor in developing his audit programs are similar to the benefits in developing and debugging any computer program. Interactive audit processing provides interactive access to report data/files and interactive execution of an audit program.

Interactive access to report data/files refers to the interrogation by the auditor of report data/files which have been stored by the system controls on files for this purpose. Examples would include frequency counts of various types of transactions on specific data in attempts to penetrate security functions.

Interactive execution of an audit program refers to the stepwise execution of an audit program providing the auditor the opportunity to examine intermediate results in-line and base the next execution step in the program on those intermediate results.

The working group has concluded that interactive techniques for auditing has not been wide spread. The reasons identified include: (1) Interactive audit programs are not widely available and auditors are not accustomed to operating in this mode. (2) Interactive access to report data/files requires that controls be built into systems to collect these data and to create the report files. The needed controls have not been formalized sufficiently to provide for extended auditability. (3) Interactive execution of an audit program requires new software design for the auditor to use. Few such processors exist and those that do exist have not received sufficient acceptance and exposure.

## 1.4 Benefits of Interactive Tools and Techniques

A number of benefits can be derived from the use of interactive tools and techniques to facilitate the performance assurance function. Since their cost effectiveness has not been fully explored, further research and evaluation is warranted.

Interactive tools and techniques facilitate the focusing on system or control functions in as much detail as is needed (Zoom lense effect). They allow the review of events in near real-time, through continuous updating of audit trails and recorded events. This provides the capability to:

- -Screen for file status conditions.
- -Determine exception conditions.
- -Summarize relevant data or conditions.
- -Display unusual conditions.

They may improve audit effectiveness by providing additional capabilities for determining characteristics and usage of controls.

They may increase or improve the efficiency of audit by allowing more immediate return on audit effort.

They improve timeliness of auditing through provision of immediate feedback and allow corrective action to occur without delay, thus reducing exposures.

They reduce clerical effort and audit preparation and allow the auditor to devote more time to professional effort and analysis.

## 1.5 Further Deliberation and Research

The group feels that further deliberations and research are required in the following areas:

- -Specification of design and performance requirements for interactive audit tools and techniques.
- -Designs of interactive audit tools and techniques for interfaces with operating systems and data base management systems.
- -Behavioral audit research to study audit behavior in an interactive

human-machine mode of operation.

- Development of a comprehensive audit and control theory to guide Performance Assurance (PA) professionals in their activities and software designers in the development of appropriate audit tools and techniques.

## 2. GOAL, OBJECTIVES, DEFINITIONS

### 2.1 Goal

The development of an auditing approach for the use of on-line or interactive techniques to achieve performance assurance in computer systems.

### 2.2 Objectives

- Define the scope and requirements for interactive tools and techniques.
- Review and define auditability and control characteristics in computer systems.
- Describe tools and techniques available and specify needed ones.
- Develop criteria for the use of these tools in specific systems environments and define the required interfaces (e.g. with Data Base, Operating Systems).

### 2.3 Definitions

#### 2.3.1 Performance Assurance

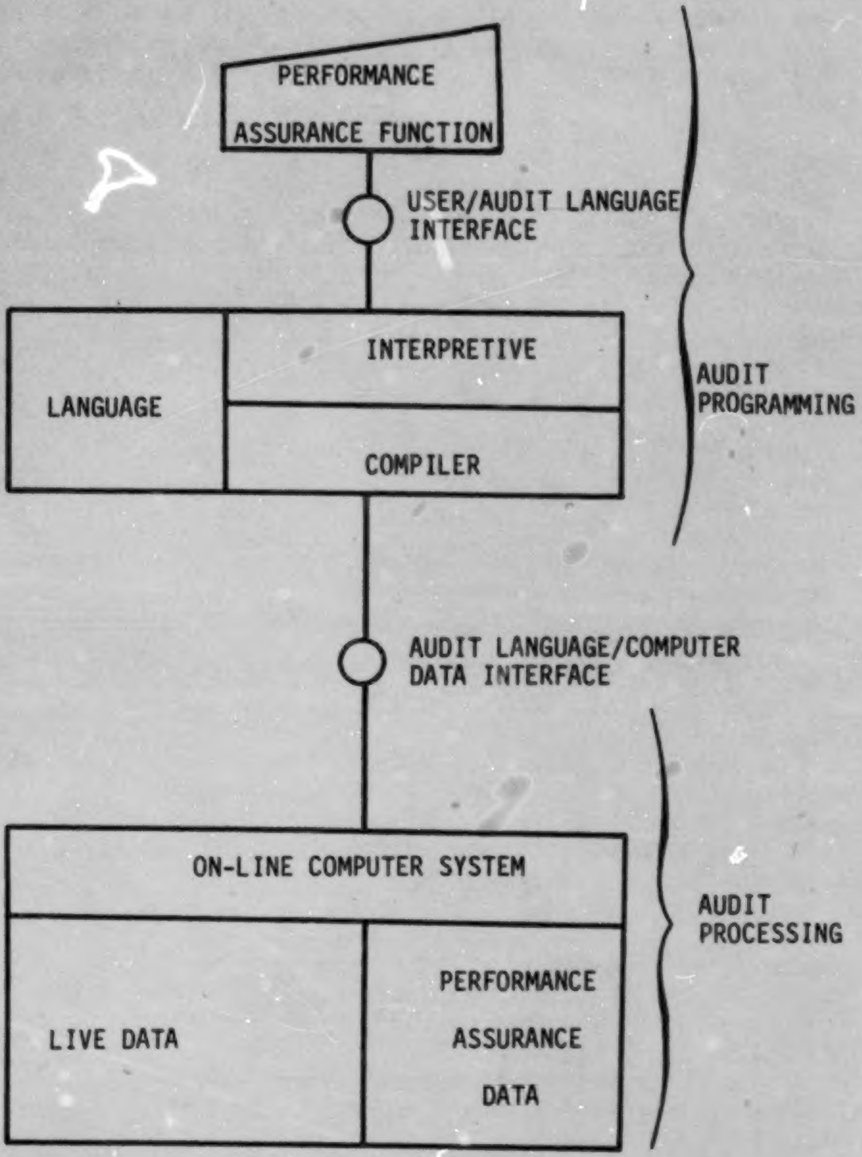
Assurance that a computer system is performing its intended functions within a specified degree of accuracy, timeliness, and data security; and that it is not performing unintended functions. The level of accuracy depends on the critical nature of the applications and files (master files, transactions and programs) as determined by management criteria.

#### 2.3.2 Interactive Tools and Techniques

Tools and techniques that provide both interactive audit programming and interactive audit processing support. As such they facilitate immediate access to or uses of live files (master files, transactions and programs) and to performance assurance data. This includes interactive access to application and control files as well as continuous dialogue between human and computer systems. (See Figure 1.)

#### 2.3.3 Interactive Audit Programming

The development of a computer audit program by means of a language, i.e. the auditor gets immediate feedback from the language on syntactic errors and preferably semantic errors as well - such that the audit program is instantaneously debugged and ready for immediate (or deliberately delayed) test and/or execution. Antonyms: generative (complier-dependent) programming, host language programming.


PERFORMANCE ASSURANCE FUNCTION
USER/AUDIT LANGUAGE INTERFACE
LANGUAGE
INTERPRETIVE
COMPILER
AUDIT PROGRAMMING
AUDIT LANGUAGE/COMPUTER DATA INTERFACE
ON-LINE COMPUTER SYSTEM
LIVE DATA
PERFORMANCE ASSURANCE DATA
AUDIT PROCESSING

INTERACTIVE AUDITING

Figure 1

### 2.3.4 Interactive Audit Processing

Interactive Audit Processing performs immediate, interpretive execution of computer audit program steps and whole audit programs against on-line files upon issuance of simple, often terminal-initiated commands.
Antonyms: Batch audit processing, Off-line file processing.

### 2.3.5 Interactive Auditing

Interactive auditing is dependent on interactive audit programming and interactive audit processing facilities as part of a "self-contained" audit software system which can be interfaced with client information systems of diverse designs.
Antonyms: Batch auditing.

### 2.3.6 On-Line Auditing

Refers to the capability to audit in an interactive manner.

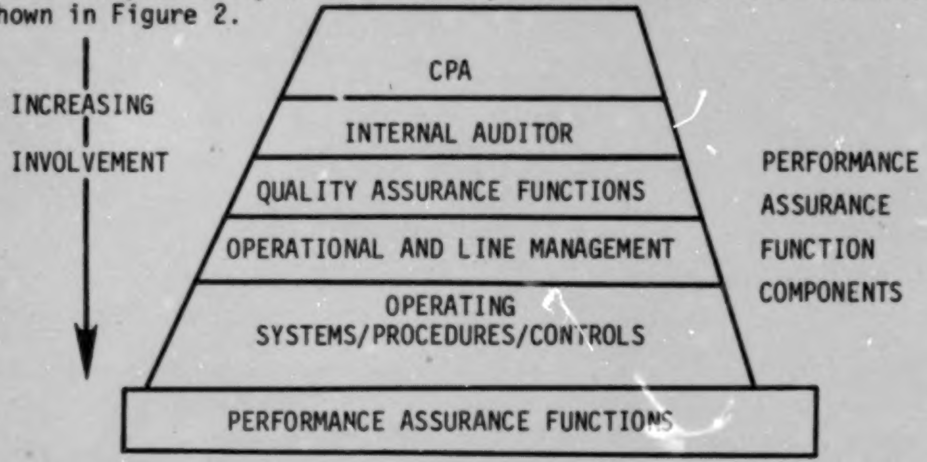
### 2.3.7 Auditing of On-Line Systems

Refers to the capability to audit both the systems themselves and their controls where the dominant mode of processing is on-line (e.g., airline reservation system, real-time process control, data entry systems, etc.)

## 2.4 Performance Assurance Functions

### 2.4.1 Model

In order to generalize the term "auditing" the group decided to illustrate the previously defined term "performance assurance functions" as shown in Figure 2.


INCREASING
INVOLVEMENT
CPA
INTERNAL AUDITOR
QUALITY ASSURANCE FUNCTIONS
OPERATIONAL AND LINE MANAGEMENT
OPERATING SYSTEMS/PROCEDURES/CONTROLS
PERFORMANCE ASSURANCE FUNCTIONS
PERFORMANCE
ASSURANCE
FUNCTION
COMPONENTS

PERFORMANCE ASSURANCE

Figure 2

### 2.4.2 CPA Functions

To review, evaluate and test an information system and its contents in performing an objective, independent examination in order to express an opinion on financial statements.

### 2.4.3 Internal Auditor Functions

To ensure that data is processed accurately and that assets are being properly safeguarded.

### 2.4.4 Quality Assurance Functions

To monitor and develop standards to insure efficient and effective management and utilization of computer resources.

### 2.4.5 Operating and Line Management Functions

To provide continuing evaluation of the development and effectiveness of management controls and degree of compliance therewith. Controls should be reviewed for:

- Effectiveness
- Completeness
- Consistency.

## 3. PERFORMANCE ASSURANCE ACTIVITIES

### 3.1 Introduction

The purpose of the performance assurance (PA) function, as previously defined, is to determine that a computer system is performing its intended functions within a specified degree of accuracy, timeliness, and data security; and that it is not performing unintended functions. The other part of the definition mentions that the level of accuracy depends on the critical nature of the applications and data as determined by management criteria.

In illustrating the activities of the various groups involved with the performance assurance function we decided, for the purpose of our deliberations, to identify the following:

- Setting PA objectives
- Gathering information
- Performing PA analyses and evaluations
- Designing and performing PA test procedures.

These activities are used in the next two sections for cross-classification purposes with existing and needed PA tools and techniques. This way it becomes possible to illustrate how the various tools and techniques can be used by professionals involved in performance assurance activities.

### 3.2 Setting PA Objectives

There are two types of objectives to be considered in performance assurance. The first type of objective relates to the nature and purpose of the performance assurance testing (audit or testing objectives). The second type of objective refers to the system to be tested. A system control objective or set of objectives are established as the basis or the framework to use in developing the system, procedures and controls for any system elements (applications). The system control objectives describe what the system is to do, i.e., in effect, the goal to be accomplished. The objectives are developed from criteria set forth by management for that particular area.

A development team, for example, in designing a system, in establishing the detailed procedures, and in determining the type and extent of internal controls to be built into the system, can relate the procedures and particularly the internal controls back to the objectives.

In situations where system control objectives have been defined, they may be also useful to the performance assurance group in evaluating the controls used in the specific system application. An end result of any design and implementation of a system, procedures and controls should include a set of documentations detailing and describing the user and the computerized internal control techniques built into that particular application. This "statement of internal control techniques" is extremely important to the performance assurance function and could be a standard for all systems.

### 3.3 Gathering Information

The information gathering phase of a performance assurance function can be described as the obtaining of all the necessary information and data needed in order to review, to evaluate or to establish systems, procedures, and controls. The material to be gathered includes, for example, the statement of internal control techniques, detailed or summary documentation, narrative descriptions of the systems and procedures, flow charts, authorization listings, and similar data. If this type of information and data is not available, it becomes necessary for the performance assurance group to develop or prepare the material for analysis and evaluation. Once the group performing the performance assurance function is required to create any or all of the data required, that group performs, in effect, functions that the systems development group should have performed. The existence of the material described above is extremely important to the performance assurance function and could be a standard for all systems.

### 3.4 Performing PA Analyses and Evaluations

The analysis and evaluation process culminates in the design and performance of tests with respect to the systems, procedures and controls. These tests may in turn, lead to further analysis and evaluation.

Two factors influence the analysis and evaluation activities: the critical nature (materiality and importance) as well as the complexity of the system application. Testing of an application becomes more extensive and more sophisticated when an application is critical and complex. In these situations, it is important for the various groups involved in performance assurance to be aware of interactive tools and techniques that are available for use in on-line testing and in testing of on-line systems. With knowledge as to when and how they can be used in the testing process, audit programs can be prepared and executed interactively. The available flexibility allows as to focus the testing on important control areas, on risk areas, and on the proper balance between compliance and substantive tests. In addition, the test programs can be prepared to utilize non-interactive tools and techniques where appropriate.

## 3.5 Designing and Performing PA Test Procedures

Based on the analysis and evaluation of the system, its procedures and controls it becomes necessary to design and test the key controls that are being relied on. This activity can be performed in the following steps:

- -Select the verification technique.
- -Determine if computer assisted techniques will be used.
- -Prepare and perform the test procedures.
- -Review test results and determine if further tests are required.

### 3.5.1 Select the Verification Techniques

In general, two approaches can be applied in verifying controls and processing:

- -Test of results: Select one or more key files or outputs of processing and confirm the results.
- -Test of processing: Perform specific tests of the critical processes and controls directly.

#### 3.5.1.1 Test of Results

Verification and testing of results is usually performed by comparisons of results with independent files, organizations or physical items or by reasonableness tests. Examples of the former would be comparison of computer records of personnel pay rates and inventory balances to independent personnel department files and to physical inventory counts. Examples of the latter would be tests of values with expected ranges or comparisons with similar information such as budgets and results of prior periods.

#### 3.5.1.2 Test of Processing

Verification of processing involves specific tools and techniques discussed in the next two sections to test specific manual and computer controls and processing steps. For example, the snapshot technique results in a list of each step of a computer program as if it is being processed and the status of key data elements as they are being modified.

### 3.5.2 Determine if Computer Assisted Techniques Will Be Used

Use of the computer will depend on:
- The nature of the control. Supervising, for example, is a control primarily tested by observation or by review of documented supervisory actions. Integrity tests of a data base may, conversely, require the use of a computer.
- Availability of computer files and processing time.
- Cost justifications.
- Computer skills to develop a computer program, if needed.

### 3.5.3 Prepare and Perform Test Procedures

The preparing and performing of the test procedures are themselves subject to controls. The controls must ensure that the programs and procedures are designed to achieve the desired test objectives and that the procedures and files are used as specified. Commonly, compliance and substantive tests are distinguished although they tend to overlap and the same test may be applied both for the systems and for the data tests respectively.

Substantive auditing relates primarily to the financial statements as of the end of a fiscal year. Substantative tests are applied to the verification of dollar values and financial balances rather than the verification of internal control. Their extent is governed by the reliance on internal controls as determined by compliance tests.

### 3.5.4 Review Test Results and Determine if Further Tests Are Required

This step is an analysis and evaluation function to ensure that the test results are valid. It assumes that the test methodology, procedures and results are documented for subsequent, independent review in a final evaluation of controls and related reliance and exposure.

The end result of performance assurance is the determination whether and to what extent reliance can be placed on the system and the results of system processing. While the conclusions reached by the separate groups may differ to some extent, they each review the results of the testing to estimate system reliability in reaching their respective conclusions.

## 4. EXISTING PERFORMANCE ASSURANCE TOOLS AND TECHNIQUES

### 4.1 Introduction

In an attempt to review existing performance assurance (PA) tools and techniques in the context of the previously identified PA functions, traditional batch and interactive tools and techniques were identified separately. These are summarized in Figure 3.

On each of these, brief comments are offered in terms of advantages and disadvantages, although no attempt is made to exhaust the classification possibilities. The major purpose of the exercise was to identify gaps for needed PA tools and techniques that are discussed in section 5.

## 4.2 Batch PA Tools and Techniques

### 4.2.1 Utility Programs

Programs provided by or acquired from hardware vendors and software companies to facilitate efficiency, utilization, monitoring and documentation. Because of the vast number of these, a short list may suffice to illustrate the variety of these systems:

- -SMF (Systems Management Facility)
- -Automated Flow Charting Systems
- -Data Dictionaries
- -Program Dictionaries
- -Library Systems for data and programs
- -HMBLIST (utility to detect IBM O/S modifications)
- -Comparison systems (source to object)

a. Advantages
   1. May be available at no or low cost.
   2. Provides additional facts for auditors and allows the auditor to probe into computer systems beyond a data file and transaction orientation.

b. Disadvantages
   1. May require additional technical expertise, (i.e. operating systems, DBMS, etc.)
   2. Not tested and implemented as "audit tools".

### 4.2.2 Test Decks

Hypothetical transactions and work file records designed to test the controls and accuracy of program logic.

a. Advantages
   1. Provides a highly specific test of individual control features and exception conditions.

b. Disadvantages
   1. Difficult to develop and maintain test data due to program modification.
   2. Requires special computer runs unless a test module is available.
   3. Seldom comprehensive enough to provide an adequate test of reports and statistics. An audit standard should be that test data is never posted to live files.

### 4.2.3 Audit Modules

Special audit subroutines are sometimes contained in application programs to perform specific audit functions such as an aging of accounts or to eliminate the impact of test data on the printed reports (see ITF on the following page).

a. Advantages

        1. Provides for the execution of special audit tasks if required.
        2. Can be "triggered" at any time.
    b. Disadvantages
        1. Require expert programming and, depending on the design, special operating procedures.
        2. May be invoked by non-authorized personnel.

### 4.2.4 ITF (Integrated Testing Facility)

Means of passing test transactions through a computer system simultaneously with live transactions without adversely affecting live files or outputs. A separate set of outputs, including statistics and reports, are produced for a minicompany. This not only ensures that the test material does not interfere with any outputs concerning the real company, but also enables the auditor to check that statistics and reports are being prepared correctly.

a. Advantages
    1. Testing in a live environment routinely.
    2. No special running time required.
    3. No effect on live records.
    4. Provides reports and statistics.
b. Disadvantages
    1. Difficult to produce and maintain a complete set of test data.
    2. Requires special programming to integrate the test subsystem with the live system.

### 4.2.5 Test Data Generator

A computer method to generate hypothetical transactions for testing purposes.

a. Advantages
    1. Automated development of test transactions and work file records.
b. Disadvantages
    (See Test Decks)

### 4.2.6 Snapshot

Technique of capturing the status of data at a particular point in time of the producing cycle, e.g., triggered by specific transaction types, that are identified by "tags" (tagging).

a. Advantages
    1. A good method for a very specific purpose.
    2. May reduce "logging" requirements.
b. Disadvantages
    1. Requires frequent monitoring by auditor to avoid "over-tagging".
    2. May be too limited for general audit applications and may affect proper "logging" procedures negatively.

### 4.2.7 Tracing

A technique to identify the sequence of actual exceptions of program code, triggered by specific transaction types - identified by "tags" - on conditions (as under Snapshot)

a. Advantages
   (as under Snapshot)
b. Disadvantages
   (as under Snapshot)

### 4.2.8 SCARF (System Control Audit Review File)

Incorporation of auditor - determined reasonableness tests into normal data processing applications for the purpose of tagging and/or extracting exceptional data into audit files.

a. Advantages
   1. Continuous exception reporting (see Audit Modules)
b. Disadvantages
   1. Processing time

### 4.2.9 Audit Software Packages

High-level, data processing languages to provide data access and computational manipulations in addition to specific audit functions such as aging, confirmations, sampling, etc. The functions performed by the various software packages are not all equivalent in terms of:

-capabilities, i.e., computation, sampling, compares, etc.
-interfacing with data (i.e., DBMS and file structures);
-efficiency of execution (i.e., running time, auditor preparation, etc.)

a. Advantages
   1. Provides independent data gathering and analysis of data files.
   2. Improves efficiency of auditor time and can assist in expanding the scope of audits.
   3. Provides access to the entire universe of data.
b. Disadvantages
   1. Processing time can be longer than use of standard programming languages.

A standard should be that all audit software packages should be restricted to a read-only mode.

### 4.2.10 Parallel Simulation

It is a means of testing computer application processing by using the same input data and files as the application systems and attempting to produce the same results. The simulation results are compared to "live" results confirming the results of computer applications processing or identifying areas of descrepancies for further analysis.

a. Advantages
   1. Compliance testing of application programs can be performed with live data without jeopardizing files.
   2. Application program functions tested can be analyzed primarily through non-technical user documentation (error and

balancing procedures).

b. Disadvantages
  1. Requires good knowledge of functions performed.
  2. Time required to develop simulation program.

### 4.3 Interactive PA Tools and Techniques

The group identified two interactive audit tools available to date and suggests that these be further studied and evaluated. We also followed two additional leads to what were supposedly other existing interactive audit tools, but these proved to be unsuccessful.

### 4.3.1 ACL (Audit Command Language)

ACL is available in two versions at the University of B.C. in Vancouver, B.C. The first is running under the Michigan Terminal System (MTS Operating System) and is used extensively in teaching (both academic and professional through CICA) and research. The IBM version runs under the IBM/OS/VS1 system and is used by internal and external auditors as well as consultants. As the first fully interactive audit language, ACL represents a pioneering effort to combine the various performance assurance functions into a single professional user language.

### 4.3.2 NAARS (National Automated Accounting Research System)

NAARS has been developed jointly by the AICPA and Mead Data Central, Inc. It is possible to search interactively (through a computer terminal) the full text of the financial statements, footnotes and auditor reports from the published annual reports to shareholders of over 3,500 companies. Other files accessible are various AICPA publications as well as federal securities law and federal trade regulations.

## 5. NEEDED PERFORMANCE ASSURANCE TOOLS AND TECHNIQUES

### 5.1 Introduction

The mentioned performance assurance (PA) tools and techniques that are in existence to date are, in many cases, quite useful in an auditing situation. However, these tools are in many instances little utilized by both auditors and quality assurance personnel. Their potential may be unknown, or their applicability to performance assurance may not be obvious. In some instances the tools are designed for another purpose (e.g. hardware or software monitors) and their applicability to security or performance assurance is not intuitively obvious.

The following subsection describes and explains categories of needed tools and specifies requirements for their design and development.

## 5.2 Needed Tools and Techniques

The tools and techniques described below can be utilized in two major areas. Detection of malfunctions or inadequacies of systems, procedures, or controls can be accomplished interactively through monitoring, trace or test facilities. It is also possible to measure the "health" of a system looking for symptoms such as excessive errors, anomalous access to a sensitive file or excessive changes to a given program. This is analogous to the tests, probes and data gathering performed by the medical profession to diagnose disease and requires analogous judgments by PA professionals.

### 5.2.1 Near Real-Time Error Detection and Correction

The tools in this category are useful in detecting and when practical, correcting errors in computer systems as they occur before any"damage" has occurred. Examples of damage include the incorrect automatic disbursement of large amounts of funds in a funds disbursing system or false feedback in a process control system. These controls are oriented to the operational system "in the whole". It is assumed that the hardware and individual system modules have already been tested and verified, but that failures may occur when the various subsystems are operating together as a larger system. We submit that the following tools are needed:

- Interface Data Monitoring and Testing - routines that exist to test data at each interface between modules in a system in terms of range, limits, and validity of fields.
- Threshold Detection - hardware and software monitors to measure variant and invariant characteristics of systems to detect and immediately abort in cases of unusual usage patterns.

### 5.2.2 Monitoring of Adequacy of Controls

The tools in this category provide for the on-line testing of the predetermined and specified controls that have been built into the system. They permit the auditor to perform tests on the operational system to detect potential trouble spots. We submit that the following tools are needed:

- Software Behavior Monitoring - these routines would exist in a dormant state in a system and when invoked by an auditor would begin monitoring the behavior of specified software modules in terms of accesses, inputs, outputs, and frequency of usage.
- Configuration Auditing - through access to this routine, the auditor can instantly get information on the current configuration of the operational system for particular use in large teleprocessing systems.
- Interactive Tracing - routines similar to generalized debug packages can allow an auditor to step through the operational cycle of a system, monitoring both changing data values and synchronization of events, and making modifications to data values to verify the adequacy of controls at the module interfaces.
- Artificial Load Generators - routines to permit the auditor to generate controlled amounts of transactions and input data to test the

system under varying conditions of loading.

### 5.2.3 Measurement of Design Accuracy

In this section we address tools and techniques for specifying and documenting systems and controls. It is possible to verify system specifications against functional requirements for systems as well as system controls.

We submit that the following tools are needed:

- -Requirements Specification Languages - computer languages for specifying system requirements to permit verification against functional requirements.
- -Control Feature Specifications - formal methods for programmers to document control features such that auditors can "easily" understand their applications, function, and anticipated performance.

### 5.2.4 Program Modification Control

The tools in this category would permit the auditor to verify the adequacy of the procedures for controlling program modifications through on-line testing.

We recommend the following tools:

- -Program Modification Detection - check sums and similar routines can be used to detect modification of systems, applications and control software.
- -Program (Modification) Audit Trails - through interrogating a particular on-line file the auditor could get complete information on every program. In addition, it should be possible to recognize changes to a particular program, including who made each change, when it was made, the problem that caused the change, and when the modified program became operational.

### 5.2.5 Monitoring System Trouble Indicators

The tools in this category would permit an auditor to interrogate files containing information on the execution of and system control of various security features. The recommended needed tools are:

- -Utilization Frequency Monitoring - provides frequency information, on-line, concerning accesses to any priviledged module, device, data, and transaction.
- -Utilization of Control and Security Features - interrogation of this file would allow an auditor to obtain information on the utilization of any security, control, error detection, or error correction feature in the system including frequency of usage and results of execution; an example would be information on data before and after execution of an automatic error detection feature.

| | PERFORMANCE ASSURANCE FUNCTIONS | | | | |
|---|---|---|---|---|---|
| | | | | Testing | |
| TECHNIQUES AND TOOLS | Control Objectives | Information Gathering | Analysis & Evaluation | Compliance | Substantive |
| 1. Batch PA Tools & Techniques | | | | | |
| a. Utility Programs Documentation | X | X | X | | |
| Flow Charting | | X | X | X | |
| Access Authorization Table | | X | | X | |
| Data Dictionary | X | X | X | X | |
| Program Dictionary | X | X | X | X | |
| Compare-Source/Object Programs | | X | X | X | |
| Check Sum | | X | X | X | |
| SMF | | X | | X | X |
| b. Test Deck | | | | X | |
| c. Audit Modules | | X | X | X | X |
| d. ITF | | | | X | |
| e. Test Data Generator | | X | | X | |
| f. Snapshot | | X | | X | |
| g. Tracing | | X | | X | |
| h. SCARF | | X | | X | X |
| i. Parallel Simulation | | | | X | X |
| j. Audit Software Packages | X | X | X | X | X |
| 2. Interactive Tools & Techniques | | | | | |
| a. ACL | X | X | X | X | X |
| b. NAARS | | X | X | | |

PA TOOLS & TECHNIQUES BY PA FUNCTION

Figure 3

Figure 4 summarizes the tools and techniques we feel are needed to fulfill the various performance assurance functions. A separate column "control" was added to indicate that some of these tools and techniques may also be used (already) for internal control purposes. Auditors should be aware of them to recognize their potential benefit in the information gathering function in particular.

|  | PERFORMANCE ASSURANCE FUNCTIONS |  |  |  |  |
|---|---|---|---|---|---|
| TOOLS AND TECHNIQUES | Control Objectives | Information Gathering | Analysis & Evaluation | Test-ing | Con-trol |
| Interface testing |  | X | X | X | X |
| Threshold detection |  | X | X |  | X |
| Software behavior monitoring |  | X |  |  | X |
| Configuration auditing |  | X | X | X | X |
| Interactive Trace Routine |  |  |  | X |  |
| Artificial load generation |  | X | X | X |  |
| Requirements specification | X |  | X | X |  |
| Program modification detection |  | X |  | X | X |
| Program modification audit trails |  | X |  |  | X |
| Program Modification Documentation | X | X |  |  | X |
| Utilization frequency monitor |  | X |  |  | X |
| Control specification | X | X |  |  |  |

NEEDED PERFORMANCE ASSURANCE TOOLS AND TECHNIQUES

Figure 4

## 6. SUMMARY AND RECOMMENDED FOLLOWUP

### 6.1 Introduction

This final section provides both a brief and general summary of the recognized need for interactive audit tools and techniques and offers a few recommendations for appropriate followup on the subject.

### 6.2 Need for Interactive Tools and Techniques

In spite of the apparent lack of awareness of interactive tools and techniques for performance assurance functions, the group recognizes the need for such tools and tries to summarize their benefits in the executive summary (see section 1.4).

The existing tools listed in section 4.3 deserve the attention of all professionals working in the performance assurance field and should be discussed and studied in greater depth and detail.

In identifying needed tools and techniques (see section 5) the group tries to broaden the outlook of all PA professionals and hopes to stimulate further discussion both on the auditability of modern information systems and on the ways for performing comprehensive PA audits.

### 6.3 Recommended Followup

The group feels that further deliberation and research is required. We would like to pursue the following topics as early as possible and ask for support to discuss them:

- Design criteria for interactive PA tools and techniques.
- Interface designs of interactive PA tools and techniques with operating systems (OS) and data base management systems (DBMS).
- Behavioral audit research to study interactive human-machine behavior in the context of performance assurance.
- Development of a comprehensive audit and control theory to guide PA professionals in their work and software designers in the development of PA tools and techniques.

#### 6.3.1 Design Criteria

Since a few interactive PA tools and techniques exist, it is possible to consider them as prototypes which deserve further study and evaluation by the large number of professionals active in the performance assurance field. It may be possible to adopt some of the existing tools or become feasible to specify design and performance requirements for future systems.

#### 6.3.2 Interfaces

All interactive PA tools and techniques require an interface with the operating system and many of them will require an interface with the system performing data base management functions. Yet, hardly any PA professional is involved in the design and standardization of OS and DBMS. Differences in OS and DBMS or inherent weaknesses of any one of these may make the interfacing of PA and audit functions inefficient or ineffective. The group therefore urges all professionals to recognize the need for feasible interface designs and urges them to get involved in deliberations concerning these important interfaces.

#### 6.3.3 Behavioral Research

Behavioral research is needed to determine which audit software functions are valuable as interactive features. Since audit requirements vary with projects and with time, some interactive tools may be relevant only in certain instances. Furthermore, under certain conditions the audit tool used may have an effect on the procedure and also on the conclusions reached by the auditors. It is therefore necessary to recognize that the audit approach may be dependent on the tool used, and vice versa. PA functions may become much easier or much more difficult, unless the interplay between auditors and their tools is recognized and studied in considerably more depth than was so far possible.

### 6.3.4 Theory

It has become feasible to develop a comprehensive audit and control theory for the performance assurance functions, because it is now possible to monitor interactive human-machine behavior in the PA context. Consequently, it will be possible to guide PA professionals in their tasks and to develop "intelligent" PA tools and techniques, thus making the performance of the various PA functions covered in this report more and more convenient and effective.

## REFERENCES

A few English references on ACL are included at the request of the editor:

1. H.J. Will, "Design of a Generalized Audit Command Language (ACL)," Lecture Notes in Economics and Mathematical Systems, M. Beckmann, G. Goos and U.P. Kuenzi (eds.), Berlin/Heidelberg/New York: Springer-Verlag, 1973, pp. 133-142.
2. H.J. Will, "An Interactive ACL (Audit Command Language) Prototype," Proceedings Session 73, Canadian Computer Conference, Edmonton, June 20-22, 1973, pp. 63-88.
3. H.J. Will, "Interactive Auditing with ACL," CAmagazine (October 1973), pp. 20-27.
4. H.J. Will, "Audit Command Language (ACL): Design Considerations and Impact on Audit Research," Proceedings Audit Research Symposium, University of Illinois at Urbana-Champaign, October 24-25, 1974, University of Illinois, 1975, pp. 53-77.
5. H.J. Will, "Audit Command Language Design: A Challenge to and Opportunity for the Profession," in H.J. Will (ed.), Legal and Technical Issues of Computer Auditing, Proceedings of a U.E.C. International Symposium on Computer Auditing, St. Augustin, June 18-20, 1975, U.E.C. and GMD, 1975, pp. 127-156.
6. H.J. Will, "Auditor/ACL Interface: Design and Behavior," Proceedings NorthWest '76 (Seattle, June 24-25, 1976), pp. 124-129.
7. Hart J. Will, Henk Brussel and Robert A. Clark, "An invitation to help develop new audit software," CAmagazine, May 1977, pp. 35-39.
8. H.J. Will and H. Brussel, "ACL: A Conversational Language for Audit Intelligence," IFIP Congress 77 Proceedings (on press).
9. H.J. Will, "ACL as a Research Tool: Suggestions for Behavioral Audit Research," Proceedings Canadian Region of the American Accounting Association, CAAS Meetings, June 1976, Quebec City, 1976, pp. 124-133.

# APPENDIX A: WORKSHOP ATTENDEE LIST

This appendix lists the Workshop attendees alphabetically. The general format of a listing is as follows with the square brackets indicating the location of the various pieces of information.

Line 1: [Name] , [Workshop Role in addition to being an attendee] [(Part of Proceedings contributed to)]

Line 2: [Job Title and/or Office Title, if known]

Line 3: [Name of Organization]

Line 4,5,...: [Address]

---

Robert P. Abbott (IX)
President
EDP Audit Controls
7700 Edgewater Drive, Suite 325
Oakland, California 94621

Donald L. Adams, Keynoter (II)
Managing Director,
Administrative Services
American Institute of Certified
Public Accountants
1211 Avenue of the Americas
New York, New York 10036

N. D. Babic (IX)
Manager of Information
Service Planning
Atlantic Richfield Company
515 South Flower Street
Los Angeles, California 90071

Sid Baurmash (IV)
Partner
Seidman & Seidman
1200 18th Street, N.W.
Washington, D.C. 20036

Robert P. Blanc (XII)
Staff Assistant
Institute for Computer Sciences
and Technology
National Bureau of Standards
Washington, D.C. 20234

Sheila Brand, Recorder (VI)
Bureau of Supplemental Security
Income Privacy Coordinator
Social Security Administration
6401 Security Boulevard
2-D-3 Oak Meadows Building
Baltimore, Maryland 21235

Dennis K. Branstad, Recorder (X)
Chairman, FIPS TG-15
Systems Architecture Section
Systems & Software Division, ICST
National Bureau of Standards
Washington, D.C. 20234

Peter S. Browne, Recorder (XII)
President
Computer Resource Controls
6 Stevens Court
Rockville, Maryland 20850

Henk Brussel (XII)
Faculty of Commerce
University of British Columbia
Vancouver, British Columbia
Canada V6T 1W5

Edmund L. Burke (VIII)
The MITRE Corporation
P. O. Box 208
Bedford, Massachusetts 01730

Richard Canning, (VIII)
President
Canning Publications
925 Anza Avenue
Vista, California 92083

Dwight Catherwood (IX)
Supervisor
Ernst & Ernst
515 South Flower Street, Suite 2700
Los Angeles, California 90071

Adolph Cecula (IV)
U. S. Geological Survey
National Center, Stop 804
12201 Sunrise Valley Drive
Reston, Virginia 22092

P. J. Corum (VI)
Assistant Chief Inspector
Bank of Montreal, Inspection
Department
129 St. James Street West
Montreal, Quebec H2Y 1L6
Canada

David L. Costello (V)
Deputy Chief Auditor-EDP
Bank of America (8-900)
315 Montgomery Street
San Francisco, California 94137

Linwood M. Culpepper (V)
Mathematician
David W. Taylor Naval Ship
Research & Development Center
Bethesda, Maryland 20084

Howard R. Davia (III)
Director of the Office of Audit
General Services Administration
19th & F Streets, N.W.
Washington, D.C. 20405

Leo Deege (XI)
Defense Audit Service
Room 624, Lynn Building
1111 North 19th Street
Arlington, Virginia 22209

Ike Dent (VI)
Director of Security & Quality
Control
Credit Bureau Inc. of Georgia
P. O. Box 4091
Atlanta, Georgia 30302

Lynne E. Devnew (X)
Financial Controls Systems
Program Manager
IBM Corporation
Data Processing Division
1133 Westchester Avenue
White Plains, New York 10604

Donald L. Eirich (V)
Associate Director, Logistics
& Communications Division
U. S. General Accounting Office
441 G Street, N. W., Rm. 5814
Washington, D. C. 20548

Jerry FitzGerald, Chairman (X)
Management Systems Consultant
Information Systems Management
Department
Stanford Research Institute
Menlo Park, California 94025
and currently with:
Jerry FitzGerald & Associates
Management Consulting
506 Barkentine Lane
Redwood City, California 94065

Thomas Fitzgerald (V)
EDP Auditor
Manufacturers Hanover Trust
4 New York Plaza
New York, New York 10015

C. W. Getz (IV)
Regional Commissioner
Automated Data & Telecommunications Services
General Services Administration
525 Market Street
San Francisco, California 94105

Malcolm Blake Greenlee, Chairman (V)
Assistant Vice President
Comptroller Division, WOS
F-31, T-20
Citibank
20 Exchange Place
New York, New York 10005

Peter D. Gross (VI)
Computer Sciences Corporation
6565 Arlington Boulevard
Falls Church, Virginia 22046

Thomas L. Hamilton (VI)
Corporate Systems Development & Services
Administrative Services Division
Eastman Kodak Company
Rochester, New York 14650

Carl Hammer, Chairman (VI)
Director, Computer Sciences
Sperry UNIVAC Computer Systems
2121 Wisconsin Avenue, N.W.
Washington, D.C. 20007

Robert V. Jacobson, Coordinator
Assistant Vice President
Chemical Bank
55 Water Street
New York, New York 10041

S. Jeffery, Host (I,III)
Chief, Systems & Software Division
Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D.C. 20234

Stuart W. Katzke, Recorder (IX)
Systems Architecture Section
Systems & Software Division, ICST
National Bureau of Standards
Washington, D.C. 20234

Walter Kennevan (IV)
Director, MIS Program
Room 206, Hurst Hall
College of Public Affairs
American University
Washington, D.C. 20016

Kathleen Kolos, Recorder (IV)
CIA
OS/ISSG
Washington, D.C. 20505

Leonard I. Krauss, Chairman (IX)
Manager, Management Consulting Service
Ernst & Ernst
140 Broadway
New York, New York 10005

Milton Lieberman, (X)
Group Manager
Merrill, Lynch, Pierce, Fenner & Smith, Inc.
165 Broadway
New York, New York 10006

Fred L. Lilly (III)
Lilly & Harris, CPA
1113 Williamson Building
Cleveland, Ohio 44114

Theodore A. Linden, Recorder (VIII)
Systems Architecture Section
Systems & Software Division, ICST
National Bureau of Standards
Washington, D.C. 20234

Thomas C. Lowe, Coordinator
Chief, Systems Architecture Section
Systems & Software Division, ICST
National Bureau of Standards
Washington, D. C. 20234

Don C. Lundberg (VIII)
IBM Corporation
1501 California Avenue
Palo Alto, California 94304

Aileen MacGahan (IX)
Assistant Treasurer
Chase Manhattan Bank
1 Chase Plaza - 21st Floor
New York, New York 10015

W. Gregory McCormack II (VII)
Senior Electronic Systems Auditor
Western-Southern Life
400 Broadway
Cincinnati, Ohio 45202

Herman McDaniel (IV)
Director, ADP User Education
The ADP Management Training Center
U. S. Civil Service Commission
Washington, D.C. 20415

Robert G. McKenzie, General Chairman
(Co-editor)
Audit Manager, Logistics &
Communications Division
U. S. General Accounting Office
441 G Street, N. W., Room 5814
Washington, D.C. 20548

Philip M. McLellan (XI)
Manager, EDP Security Branch
Royal Canadian Mounted Police
720 Belfast Road
Ottawa, K1A 0R2
Canada

Wallace R. McPherson, Jr., Recorder
(V)
Director, HEW ADP Standards &
Security Programs
HEW OMT (Room 551 D)
200 Independence Avenue, S.W.
Washington, D.C. 20201

Gerald E. Meyers (III)
Manager, Internal Audit & President
EDP Auditors Association
CNA Insurance
333 South Wabash
Chicago, Illinois 60604

James F. Morgan (VI)
GE Information Service
401 N. Washington Street
Rockville, Maryland 20850

Robert Morris (X)
AT&T (Room 545782)
295 North Maple Avenue
Basking Ridge, New Jersey 07920

William Hugh Murray, Chairman (VII)
Senior Market Support Administrator
IBM Corporation
1133 Westchester Avenue
White Plains, New York 10604

Eldred Nelson (VII)
TRW Systems Group
1 Space Park
Redondo Beach, California 90278

Albrecht Neumann, Recorder (XI)
Computer Science Section
Systems & Software Division, ICST
National Bureau of Standards
Washington, D.C. 20234

Hubert S. Obstgarten (IX)
Manager
Ernst & Ernst
1300 Union Commerce Building
Cleveland, Ohio 44115

Kenneth T. Orr (VII)
Vice President
Langston, Kitch & Associates
715 East 8th
Topeka, Kansas 66607

John Panagacos, Coordinator
Manager, Data Base Protection
Equitable Life
1285 Avenue of the Americas
New York, New York 10019

William E. Perry, Chairman (III)
Director of EDP and Research
The Institute of Internal
Auditors, Inc.
International Headquarters
Altamonte Springs, Florida 32701

Harold J. Podell (VIII)
Audit Manager
Logistics and Communications Division
U. S. General Accounting Office
441 G Street, N.W., Room 5814
Washington, D.C. 20548

Kenneth A. Pollock (III)
Assistant Director for ADP
Financial & General Management Studies Division
U. S. General Accounting Office
441 G Street, N.W., Room 6011
Washington, D.C. 20548

Gerald J. Popek (VI)
University of California-LA
3532 Boelter Hall
405 Hildgard Avenue
Los Angeles, California 90024

Susan K. Reed, Recorder (VII)
Systems Architecture Section
Systems & Software Division, ICST
National Bureau of Standards
Washington, D.C. 20234

Harry Robinson (XI)
Vice President
Metropolitan Life
One Madison Avenue
New York, New York 10010

Robert S. Roussey (XII)
Partner
Arthur Andersen & Company
1345 Avenue of the Americas
New York, New York 10019

Zella G. Ruthberg, General Vice Chairman (Co-editor)
Systems Architecture Section
Systems & Software Division, ICST
National Bureau of Standards
Washington, D.C. 20234

Frank S. Sato (III)
Deputy Assistant Secretary of Defense (Audit) and Director, Defense Audit Service
Lynn Building, Suite 607
1111 North 19th Street
Arlington, Virginia 22209

Donald L. Scantlebury (III)
Director, Financial & General Management Studies Division and President, Association of Government Accountants
U. S. General Accounting Office
441 G Street, N.W., Room 6001
Washington, D.C. 20548

Barry S. Silverman (IX)
Manager of Internal Audit, EDP
Gulf & Western Industries, Inc.
1 Gulf & Western Plaza
New York, New York 10023

C. O. Smith, Chairman (IV)
Assistant Director, Logistics and Communications Division
U. S. General Accounting Office
441 G Street, N.W., Room 5814
Washington, D.C. 20548

Michael J. Sopko (XI)
GTE Service Corporation
1 Stamford Forum
Stamford, Connecticut 06904

Carl Spencer (VIII)
Glendale Federal Savings & Loan Association
401 N. Brand Blvd.
Glendale, California 91209

Fred A. Stahl
Assistant Professor
Electrical Engineering and Computer Science
Columbia University
1312 Mudd Building
New York, New York 10027

Norman Statland (XI)
Partner
Price Waterhouse & Company
1251 Avenue of the Anericas
New York, New York 10020

T. Q. Stevenson, Recorder (III)
U. S. Department of Agriculture (ADS)
Room 4141-S
Washington, D.C. 20250

Robert Stone (XI)
Uniroyal Corporation
Oxford Management and Research
Center
Middlebury, Connecticut 06749

Ken Sussman (X)
Supervisor
Bell Laboratories
Holmdel, New Jersey 07733

Stephen T. Walker (VI)
Program Manager
Defense Advanced Research
Projects Agency
1400 Wilson Boulevard
Arlington, Virginia 22209

Joseph J. Wasserman (XII)
J. J. Wasserman & Company
11 Rock Spring Avenue
West Orange, New Jersey 07052

Douglas Webb (VIII)
EDP Audit Controls
7700 Edgewater Drive, Suite 325
Oakland, California 94621

Richard D. Webb, Chairman (XI)
Touche Ross & Company
1633 Broadway
New York, New York 10019

Clark Weissman, Chairman (VIII)
System Development Corporation
2500 Colorado Avenue
Santa Monica, California 90406

Barry Wilkins (VII)
Manager, Audit DP Systems and
Services
IBM Corporation
1000 Westchester Avenue
Harrison, New York 10604

Hart J. Will, Chairman (XII)
Faculty of Commerce
University of British Columbia
2075 Wesbrook Place
Vancouver, British Columbia
V6T 1W5
Canada

Ronald L. Winkler (VI)
Associate Attorney
Sutherland, Asbill & Brennan
1666 K Street, N.W.
Washington, D.C. 20006

Donald R. Wood (XII)
Partner
Touche Ross & Company
111 East Wacker Drive
Chicago, Illinois 60045

# APPENDIX B: EVOLUTION OF THE WORKSHOP AND PROCEEDINGS

## 1. INITIATING THE WORKSHOP

The National Bureau of Standards initiated Task Group 15 (TG-15) within the Federal Information Processing Standards (FIPS) program in 1973 to develop standards in Computer Systems Security. TG-15, chaired by Dennis K. Branstad of NBS, was composed of representatives from private industry as well as Federal, State and local governments. In March of 1976 an informal task team on Guidelines for Computer Security Auditing was formed within TG-15. It was chaired by Robert G. McKenzie of the General Accounting Office and had Zella G. Ruthberg as the NBS liaison person. Its mission was to be two-fold: 1) to convene a workshop on security auditing that would consolidate the state-of-the-art information available in the field and define areas for future research and 2) to adapt this information to the needs of Federal agencies in the form of Federal Information Processing Guidelines. The Invitational Workshop on Audit and Evaluation of Computer Security, which took place on March 22-24,1977 in Miami Beach, Florida, accomplished the first of these two tasks. Since TG-15 was terminated as a formal committee in the Spring of this year, the second task is expected to be accomplished by a working group convened for this purpose and will result in a FIPS Guideline publication by the National Bureau of Standards.

## 2. PLANNING THE WORKSHOP

Under Robert McKenzie's direction and Zella Ruthberg's assistance, the TG-15 task team worked on developing what was hoped would be a productive format and a comprehensive set of topics for the workshop. It was an informal group consisting of Peter S. Browne of Computer Resource Controls, Adolph Cecula of the U.S. Geological Survey, Robert H. Courtney of IBM, Frank Drefs of HEW, Robert V. Jacobson of Chemical Bank, John Panagocos of Equitable Life, and Harry Robinson of Metropolitan Life.. Inputs on possible topics were contributed by the task team members as well as requested and received from William E. Perry of the Institute of Internal Auditors, Robert L. Stone of the American Institute of Certified Public Accountants, and Keith Dorricott of the Canadian Institute of Chartered Accountants.

## 2.1 Workshop Format

The format decided upon was a relatively small invitational topic-area workshop that would cover ten major areas of concern in computer security audit. Each topic would be handled by an interdisciplinary group of not more than ten individuals. It would be chaired by a recognized authority in that area and staffed with a broad range of experts mainly selected by its chairman. A concerted effort would be made to obtain representation from both the audit and computer communities. The job of Recorder for the various sessions was assigned to task team members and NBS people. During the Workshop the Recorders were responsible for capturing and distributing in printed form major ideas developed in their sessions. Some Recorders, by mutual agreement, did much more than that. A few task team members were to be session coordinators as well as provide a pool of back-up attendees for last minute drop-outs. Robert McKenzie was to be the General Chairman and Zella Ruthberg the General Vice Chairman. This last arrangement provided the vehicle for the excellent support given this workshop by both GAO and NBS.

Each session was to spend over two days developing a position paper on their topic. If no consensus could be reached a majority and minority report was requested. The last afternoon was set aside for the presentation of conclusions by the chairman of each session. The results of these discussions would be published by NBS in a Proceedings. It should be noted that this format was patterned after the highly successful NBS Workshop on Data Base Directions held in October of 1975.

## 2.2 Workshop Topics and Chairmen

It was recognized that no set of topics could be selected to cover the main areas of the subject and also be mutually exclusive. There would be unavoidable overlapping with any set of topics. The actual topic selections by the task team were ultimately made from the point of view of covering the major considerations in any computer security audit.

The topic areas and the selected chairmen were as follows:

| | |
|---|---|
| INTERNAL AUDIT STANDARDS.......... | William E. Perry<br>Institute of Internal Auditors |
| QUALIFICATIONS AND TRAINING....... | C. O. Smith<br>U. S. General Accounting Office |
| SECURITY ADMINISTRATION........... | Blake Greenlee<br>Citibank |
| AUDIT CONSIDERATIONS IN VARIOUS SYSTEM ENVIRONMENTS............... | Carl Hammer<br>Univac |
| ADMINISTRATIVE AND PHYSICAL | |

| | |
|---|---|
| CONTROLS | W. H. Murray<br>IBM |
| PROGRAM INTEGRITY | Clark Weissman<br>System Development Corporation |
| DATA INTEGRITY | Leonard I. Krauss<br>Ernst & Ernst |
| COMMUNICATIONS | Jerry FitzGerald<br>Stanford Research Institute |
| POST-PROCESSING AUDIT TOOLS AND TECHNIQUES | Richard D. Webb<br>Touche Ross & Co. |
| INTERACTIVE AUDIT TOOLS AND TECHNIQUES | Hart J. Will<br>University of British Columbia |

### 2.3 Pre-Workshop Session Activities

Each chairman, with guidance from the General Chairman and Vice-Chairman, then proceeded to fill his session with a balance of individuals from the audit and computer communities. A more elaborate description was written for each of the session topics and distributed to all prospective participants to enable them to come to the workshop with a clearer idea of the subject of their session. Session chairmen were asked to request and distribute pre-workshop position statements from their participants in order to stimulate their group to formulate some of their ideas prior to the workshop. Many participants prepared such pre-workshop statements so that in general the convened sessions were able to progress very rapidly. Each session chairman was given complete freedom to structure his session in any way he felt might be productive. This proved to be a useful tactic since it gave each chairman and his attendees the latitude of being able to operate in a manner they were most comfortable with.

## 3. AT THE WORKSHOP

After the keynote address had set the stage for the activities of this Workshop, the individual sessions each met separately for two and one half days to develop their thoughts on each of their topics. Each session had a Chairman, a Recorder, and four to eight attendees. They were supplied with a folder for each, containing a copy of FIPS PUB 39 ("A Glossary of Terminology for Computer Systems Security"), the Canadian Treasury Board Guide on EDP Administration entitled "Security in an EDP Environment," plus various writing materials to make things convenient. The Workshop office at the meeting site supplied the sessions with continuous typing and xerox services to expedite matters. On the last afternoon of this three-day effort the attendees again met as a single group and each session reported its findings. At the end of the Workshop eight of the sessions submitted a rough draft of their report and two submitted detailed outlines.

## 4. THE SESSION REPORTS

The session attendees were given a great deal of latitude in producing their session reports with the result that no two reports were produced in exactly the same way. In some cases the writing of the report was divided among all the attendees at that session. In other cases an individual or a small group from the session wrote the report. In most cases the written report was reviewed by all the members of the session. Although the attendees of each session were given the option of producing a majority and minority report, all groups produced only consensus reports.

In presenting the reports in these Proceedings, the editors introduced an Editors' Note at the beginning of each report. This contains a brief biography of the session Chairman and a statement of the complete charge given to that session. Included at the end of this Editors' Note is a brief statement concerning the manner in which that report was produced.

☆ U. S. GOVERNMENT PRINTING OFFICE : 1977—240-848/336

NBS-114A (REV. 7-73)

| | | | |
|---|---|---|---|
| U.S. DEPT. OF COMM.<br>**BIBLIOGRAPHIC DATA SHEET** | 1. PUBLICATION OR REPORT NO.<br>SP 500-19 | 2. Gov't Accession No. | 3. Recipient's Accession No. |

4. TITLE AND SUBTITLE

*COMPUTER SCIENCE & TECHNOLOGY:*
*Audit and Evaluation of Computer Security*
*Proceedings of the NBS Invitational Workshop held at Miami Beach, Florida, March 22-24, 1977*

5. Publication Date

October 1977

6. Performing Organization Code

7. AUTHOR(S)

*Zella G. Ruthberg, Robert G. McKenzie*

8. Performing Organ. Report No.

9. PERFORMING ORGANIZATION NAME AND ADDRESS

NATIONAL BUREAU OF STANDARDS
DEPARTMENT OF COMMERCE
WASHINGTON, D.C. 20234

10. Project/Task/Work Unit No.

6401112

11. Contract/Grant No.

12. Sponsoring Organization Name and Complete Address *(Street, City, State, ZIP)*

*same as 9*

13. Type of Report & Period Covered

*Final*

14. Sponsoring Agency Code

15. SUPPLEMENTARY NOTES

Library of Congress Catalog Card Number: 77-600045

16. ABSTRACT *(A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here.)*

*The National Bureau of Standards, with the support of the U.S. General Accounting Office, sponsored an invitational workshop on "Audit and Evaluation of Computer Security," held in Miami Beach, Florida on March 22-24, 1977. Its purpose was to explore the state-of-the-art in this area and define appropriate subjects for future research. Leading experts in the audit and computer communities were invited to discuss the subject in one of ten sessions, each of which considered a different aspect. A consensus report was produced by each of the ten sessions and these reports form the body of these Proceedings. The ten topics reported on are: Internal Audit Standards, Qualifications and Training, Security Administration, Audit Considerations in Various System Environments, Administrative and Physical Controls, Program Integrity, Data Integrity, Communications, Post-Processing Audit Tools and Techniques, and Interactive Audit Tools and Techniques.*

17. KEY WORDS *(six to twelve entries; alphabetical order; capitalize only the first letter of the first key word unless a proper name; separated by semicolons)*

*Audit standards, audit techniques, audit tools, audit training, communications security, computer controls, computer security, data integrity, interactive audit, internal audit, post-processing audit, program integrity.*

18. AVAILABILITY ☒ Unlimited

☐ For Official Distribution. Do Not Release to NTIS

☒ Order From Sup. of Doc., U.S. Government Printing Office
Washington, D.C. 20402, SD Cat. No. C13.10:500-19

☐ Order From National Technical Information Service (NTIS)
Springfield, Virginia 22151

| | |
|---|---|
| 19. SECURITY CLASS (THIS REPORT)<br>UNCLASSIFIED | 21. NO. OF PAGES<br>256 |
| 20. SECURITY CLASS (THIS PAGE)<br>UNCLASSIFIED | 22. Price<br>$4.00 |

USCOMM-DC 29042-P74